

UNCLASSIFIED

AD NUMBER	
AD355386	
CLASSIFICATION CHANGES	
TO:	unclassified
FROM:	confidential
LIMITATION CHANGES	
TO:	Approved for public release, distribution unlimited
FROM:	Distribution authorized to U.S. Gov't. agencies and their contractors; Administrative/Operational Use; 24 SEP 1964. Other requests shall be referred to Office of Naval Research, Ballston Center Tower One, 800 North Quincy Street, Arlington, VA 22217-5660. NOFORN.
AUTHORITY	
31 Jan 1976, DoDD 5200.10; onr ltr 4 may 1977	

THIS PAGE IS UNCLASSIFIED

UNCLASSIFIED

AD NUMBER
AD355386
CLASSIFICATION CHANGES
TO
confidential
FROM
secret
AUTHORITY
31 Jan 1967, DoDD 5200.10

THIS PAGE IS UNCLASSIFIED

SECRET

AD 3 5 5 3 8 6

DEFENSE DOCUMENTATION CENTER

FOR

SCIENTIFIC AND TECHNICAL INFORMATION

CAMERON STATION, ALEXANDRIA, VIRGINIA



SECRET

NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

NOTICE:

THIS DOCUMENT CONTAINS INFORMATION
AFFECTING THE NATIONAL DEFENSE OF
THE UNITED STATES WITHIN THE MEAN-
ING OF THE ESPIONAGE LAWS, TITLE 18,
U.S.C., SECTIONS 793 and 794. THE
TRANSMISSION OR THE REVELATION OF
ITS CONTENTS IN ANY MANNER TO AN
UNAUTHORIZED PERSON IS PROHIBITED
BY LAW.

355386

CATALOGED BY DDC

AS AD No.

Special Handling Required
Not Releasable to Foreign Nationals

DOC
DEC 1 1964

3553



H R B - S I N G E R, I N C.
SCIENCE PARK • STATE COLLEGE, PENNSYLVANIA

SECRET

05763



DEPARTMENT OF THE NAVY
OFFICE OF NAVAL RESEARCH
WASHINGTON, D. C. 20360

IN REPLY REFER TO

SECRET

ONR:493:AS:rw
Ser: 001384
24 September 1964

SECRET - Unclassified when enclosure (1) is removed

From: Chief of Naval Research
To: Distribution List

Subj: Communications Deception for Amphibious Operations for the 1975-1980
Time Period, final report; Distribution of (U)

Encl: (1) Secret report entitled, "Communications Deception in Amphibious
Operations Area for the 1975-1980 Time Period (U)"

1. Enclosure (1), final report on subject study, is forwarded for information, comment and retention. Work leading to the publication of this report was conducted by HRB-Singer, Inc., operated under contract Nonr-4268(00) initiated in August 1963.
2. This study is one of six contracted for by the Office of Naval Research to assist in the determination and assessment of technological advances in various fields of relevance to amphibious assault operations of the 1975-1980 time period. The remaining studies cover ships and platforms, early warning, communication, tactical deception devices and techniques, and weapon systems.
3. A prime purpose in conducting these studies was to provide technological inputs to an in-house study of amphibious assault operations that was conducted and recently completed by the Advanced Warfare Systems Division, Naval Analysis Group, Office of Naval Research. The in-house study integrated these and other efforts, and formulated advanced concepts and systems in transport, combat support and command and control. Select Navy systems in support of the Landing Force were evaluated for feasibility, compatibility and utility in order to provide technical guidance to research and development planners.
4. The analytical effort covered by this report is focused upon advanced technology in deception devices and techniques (primarily communications) as it relates to amphibious operations defined in NWP-22(A).
5. The report is being released at this time because of its potential utilization by other Naval activities. Comments are elicited.


MARSHALL C. YOVITS
By direction

SECRET

DISTRIBUTION LIST

BUSHIPS

Code 300
362
363
600
670
675

BUWEPs

RM-2
RM-3
RMC
R-5
RMGA
RAAV-4
RAAV-8

CNO

OP-03
Op-06
Op-07
Op-724
Op-090
Op-91

CNR

Code 400
402
407
427
406
463
405
491
492
493 (5)

CINCPACFLT

CINCLANTFLT

COMPHIBPAC

COMPHIBTRAPAC (AWEBPAC)

COMPHIBLANT

COMPHIBTRALANT (AWEBLANT)

CMC

Code AX

AA

A02

A03

CGFMFPAC

CGFMFLANT

CGAIRFMFPAC

CMCLFDA (2)

Long Range Study Panel, MCLFDA

NAVMISCEN

NOL

NOTS/China Lake (Code 735)

NWL

Center for Naval Analyses (5)

DDC (10)

SECRET

HRB

HRB-SINGER, INC.

A SUBSIDIARY OF THE SINGER COMPANY
Science Park, State College, Pa.

483-F

**COMMUNICATIONS DECEPTION IN AMPHIBIOUS
OPERATIONS FOR THE
1975-1980 TIME PERIOD (U)**

24 January 1964

Copy No. ~~4~~ of 71 Copies

Prepared by:

*Gene Mikelonis
Richard Shearer
Edward Keller
Louis Myers
David Brown
Jewell Blankenship
W. D. Files
Don Coyne
Richard Conger*

Project Director:

Wilber D. Files

Downgraded at 3 Year Intervals;
Declassified After 12 Years
DOD Dir 5200.10

WARNING

This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. Its transmission or the revelation of its contents in any manner to an unauthorized person is prohibited by law.

Page i of viii preliminary pages
Reverse (Page ii) Blank

SECRET

ABSTRACT

This is the final report for a five-month study of communications deception in amphibious assault operations for the 1975-1980 time period. Its purpose was to identify requirements for research and development to provide the Navy with an adequate deception capability for that period.

The operational environment for assault operations in 1975-1980 is described. The U.S. philosophy of amphibious assault, anticipated capabilities for the period, and major phases in amphibious operations are discussed. The enemy philosophy of defense, reinforcement capabilities, and intelligence collection and processing methods are discussed. The state of communications technology in 1975-1980 is extrapolated from the present state of the art and is described in terms of frequency spectrum usage, modulation techniques, and operational capabilities.

Communications deception, both manipulative (transmission of false information) and imitative (intrusion into enemy nets) is discussed in terms of objectives and techniques, and jamming is also considered. Likely enemy anti-deception activities are described, and U.S. efforts to overcome these activities are considered. Finally, the threat of enemy deception activities of all types is considered in terms of its possible effects on U.S. communications deception operations.

Conclusions concerning the effectiveness of the current U.S. deception capability and the requirements for the 1975-1980 capability are presented, and a number of specific recommendations are made for research and development to assist the Navy in achieving the required 1975-1980 capability.

TABLE OF CONTENTS

	<u>Page</u>
ABSTRACT	ii
LIST OF ILLUSTRATIONS	v
I. INTRODUCTION AND SUMMARY	1
A. BACKGROUND	1
B. SCOPE OF THE STUDY	1
C. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS	2
1. Conclusions	2
2. Recommendations	3
II. THE 1975-1980 AMPHIBIOUS ASSAULT	7
A. U.S. FORCES AND OPERATIONS	7
1. The U.S. Philosophy of Amphibious Assault	7
2. New Capabilities for the 1975-1980 Period	8
3. Major Phases of Amphibious Assault Operations	10
B. ENEMY FORCES	17
1. The Soviet Philosophy of Defense Against Amphibious Assaults	18
2. Beachhead Reinforcement Capabilities	23
3. Intelligence Collection Means	24
4. Intelligence Processing Considerations	31
III. COMMUNICATIONS TECHNOLOGY, 1975-1980	39
A. USE OF THE FREQUENCY SPECTRUM	39
1. Acoustic Communications	39
2. Radio Communications	40
3. Optical Communications	42

TABLE OF CONTENTS (CONT'D)

	<u>Page</u>
B. MODULATION TECHNIQUES AND OPERATIONAL CAPABILITIES	48
IV. COMMUNICATIONS DECEPTION	53
A. MANIPULATIVE COMMUNICATIONS DECEPTION	54
B. IMITATIVE COMMUNICATIONS DECEPTION	56
1. Intrusion Techniques	58
2. Aims of Imitative Communications Deception	60
3. Requirements for Successful Intrusion	63
4. Imitative Deception Against Nonradio Communications Systems	64
C. JAMMING	65
V. ANTI-DECEPTION ACTIVITIES	71
A. DETECTION OF DECEPTION OPERATIONS	73
1. The Obtaining of New Information	76
2. The Reanalysis of Existing Information	77
3. The Changing of the Decision Threshold	78
B. ENEMY ANTI-MANIPULATIVE DECEPTION OPERATIONS	79
C. ENEMY ANTI-IMITATIVE DECEPTION OPERATIONS	80
D. U.S. EFFORTS TO OVERCOME ANTI-DECEPTION OPERATIONS	81
VI. ENEMY DECEPTION THREAT	83
VII. CONCLUSIONS AND RECOMMENDATIONS	103
A. CONCLUSIONS	103
B. RECOMMENDATIONS FOR RESEARCH AND DEVELOPMENT	106
APPENDIX: SUPPLEMENTARY INFORMATION	111

LIST OF ILLUSTRATIONS

<u>Figure</u>		<u>Page</u>
1	Block Diagram of Study Procedure	5
2	Typical Soviet Division Coastal Defense	22
3	Routing of Intelligence Information to Army Level Decision Makers	34
4	Time Required to Collect, Process, and Disseminate Information	35
5	Comparison of RF and Optical Communications Channels	43
6	Atmospheric Absorption of Optical Wavelengths	45
7	Classical Definition of Modulation Types	50
8	Geometry of Deception Situations	72
9	Testing for a Deception Operation	74
10	Jammer Requirements for Noncommunications Targets	87
11	Soviet Noncommunications Jammers	91
12	Jammer Requirements for Communications Targets	95
13	Soviet and Satellite Communications Jammers, Including Broadcast Transmitters Which Can Be Used as Jammers	99
14	Communications-Frequency Spectrum Representation of Soviet and U.S. Equipments	112
15	Soviet Communications Equipment	113
16	U.S. Jamming Equipment	119
17	Radio Net Jamming Capabilities /Soviet Nets and U.S. Jammers/	127
18	Estimated Effectiveness of Jamming and ICD against Selected Soviet Ground Units	134

I. INTRODUCTION AND SUMMARY

A. BACKGROUND

The success of an amphibious assault operation depends upon the establishment of overwhelming superiority by the assault force in the beach-head area and in the air and sea near that area. The successful establishment of a beachhead and a subsequent breakout by the assault forces can, of course, be disastrous for the enemy. And even a credible threat of an amphibious assault can cause the enemy to commit valuable personnel, weapons, and materiel to coastal defense.

Communications deception operations can be effective in helping to establish the local superiority required if the attack is to succeed. "Manipulative" deception can be used to control the information which the enemy can obtain by monitoring U.S. communications, and "imitative" deception can be used to break into enemy communications nets themselves. Both of these types of deception can be effective means of confusing the enemy as to U.S. intentions and actions, introducing false or misleading data into his intelligence systems, delaying his responses to U.S. tactical actions, and committing his forces prematurely or to the wrong areas.

The Advanced Warfare Systems Division of the Office of Naval Research, in connection with a study of amphibious warfare for the 1975-1980 time period, awarded Contract Nonr-4268(00) to HRB-Singer, Inc., on 2 August 1963 for a study of the role of communications deception in amphibious assault operations in the 1975-1980 era.

B. SCOPE OF THE STUDY

The scope of the study carried out under Contract Nonr-4268(00) is defined in the Work Statement:

The Contractor shall profile the Navy situation elements of an amphibious operation, shall delineate likely enemy operational and intelligence networks to be encountered by Navy forces including anti-deception procedures and techniques likely to be employed at each level of specificity and shall survey, project, and assess electronic deception devices and techniques potentially available to Navy amphibious forces in the time period 1975-1980. The study shall consider a wide spectrum of optical, radio and acoustic communication deception devices and techniques as well as radar jamming, spoofing and other forms of electronic

deception as appropriate from the viewpoint of technological capabilities that can be achieved and any enhancement of operational capabilities resulting from employment by a Navy amphibious force against a land area. As a corollary, an assessment of the enemy deception threat for the time period, including electronic, acoustic and visual deception devices and techniques, shall be conducted.

Because of the limited effort (one man-year) and time (five months) available for the conduct of the study, certain aspects of the problem were given heavier emphasis than others. The major emphasis was on the identification of areas where further research and development effort would be required to provide the Navy with an adequate communications deception capability for 1975-1980 amphibious assault operations. The Office of Naval Research was especially interested in the communications deception requirements which would be introduced or significantly modified due to the advancements in technology which could be expected by 1975. The use of satellites and spacecraft, for example, in surveillance and reconnaissance roles might be expected to change significantly the volume, the nature, and the timeliness of the intelligence data which the enemy might obtain concerning amphibious assault operations.

Conventional warfare with the possible limited use of nuclear weapons was considered in the study, but not an all-out nuclear war. Soviet military organization and technology were used to extrapolate the defensive capabilities for 1975-1980, and it was assumed that such a defense would be the most difficult to penetrate and that other less difficult defenses (in less developed areas of the world) would probably be derived from Soviet organization and technology.

Because of security restrictions, some of the materials upon which this study was based could be cited only in very general terms in this report.

C. SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

1. Conclusions

The U.S. naval amphibious assault forces of the 1975-1980 time frame must be prepared to operate against a wide variety of possible defenses, from fairly primitive defenses in underdeveloped nations to the first-class defenses which would be encountered on the Soviet coastline. These first-class defenses will employ sophisticated sensor systems to detect and monitor the

approaching assault forces and will be backed up by excellent intelligence data processing, weapons, and logistic support systems. The Soviet defense philosophy is one of defense in depth, involving the rapid commitment of powerful forces as soon as the intentions of the assault force becomes clear. In an assault against this type of defense, therefore, deception by the assault force can be extremely valuable. Deception could greatly extend the time required for the enemy to deduce the intentions of the attacking force, could introduce misleading data into his decision processes, and could cause him to commit his forces prematurely or to counterattack a diversionary force.

The U.S. Navy is not adequately prepared at the present time for effective communication deception operations against the first-class type of defense anticipated for the 1975-1980 period. Present techniques for manipulative deception would not be convincing to an enemy who possesses multisensor surveillance systems or fairly good direction finding capabilities or fairly effective signal analysis facilities. And the Navy capability for effective intrusion into Soviet communication nets is virtually nonexistent.

This study showed that an effective capability for manipulative deception will probably be a necessity for a successful amphibious landing against a sophisticated defense in the 1975-1980 time frame. Although strongly entrenched defenders would rely at first primarily on nonradio communications, a capability for imitative deception would be an extremely valuable tool in achieving a break-out once the assault forces are ashore and the situation becomes more fluid. But considerable research and development effort will be required if these capabilities are to be achieved.

2. Recommendations

A number of specific areas for investigation, research, and development became apparent during the course of the study. In general, much heavier emphasis must be placed upon communications deception. In the 1975-1980 period deception techniques must be much more sophisticated than they are today if they are to be successful, and a poor deception effort may be worse than none at all. Furthermore, communications deception must be integrated with other forms of deception because of the increased sophistication of 1975-1980 surveillance and intelligence systems. More information is needed concerning these systems so that the overall U.S. communications deception effort can be given accurate and efficient direction.

With respect to manipulative deception (transmission of false or misleading information), the study identified the following requirements for further investigation:

- (1) Techniques for the deception of multisensor surveillance and reconnaissance systems
- (2) Techniques to improve the authenticity of prerecorded communications transmissions used in deception
- (3) Techniques for the neutralization or destruction of enemy surveillance and reconnaissance systems
- (4) Enemy communications intelligence techniques, especially their time requirements
- (5) Procedures and techniques for the generation and transmission of false information
- (6) Procedures and techniques for the operation of dummy traffic nets and the insertion of this traffic in other nets
- (7) Techniques for underwater acoustic communications deception
- (8) Continued improvement of capabilities for transporting amphibious assault forces
- (9) Techniques for modification of weather conditions or the generation of artificial weather.

With respect to imitative deception (insertion of false information in enemy communications nets), the study identified the following requirements for further investigation:

- (1) Training and assignment to deception units of personnel who possess a good knowledge of the enemy language and culture
- (2) Techniques for intrusion into enemy wire and landline nets
- (3) Development of communications equipment with signal characteristics like those of enemy equipment
- (4) Development of lock-on and tracking techniques for laser communications
- (5) Psychological warfare techniques for use in intrusion.

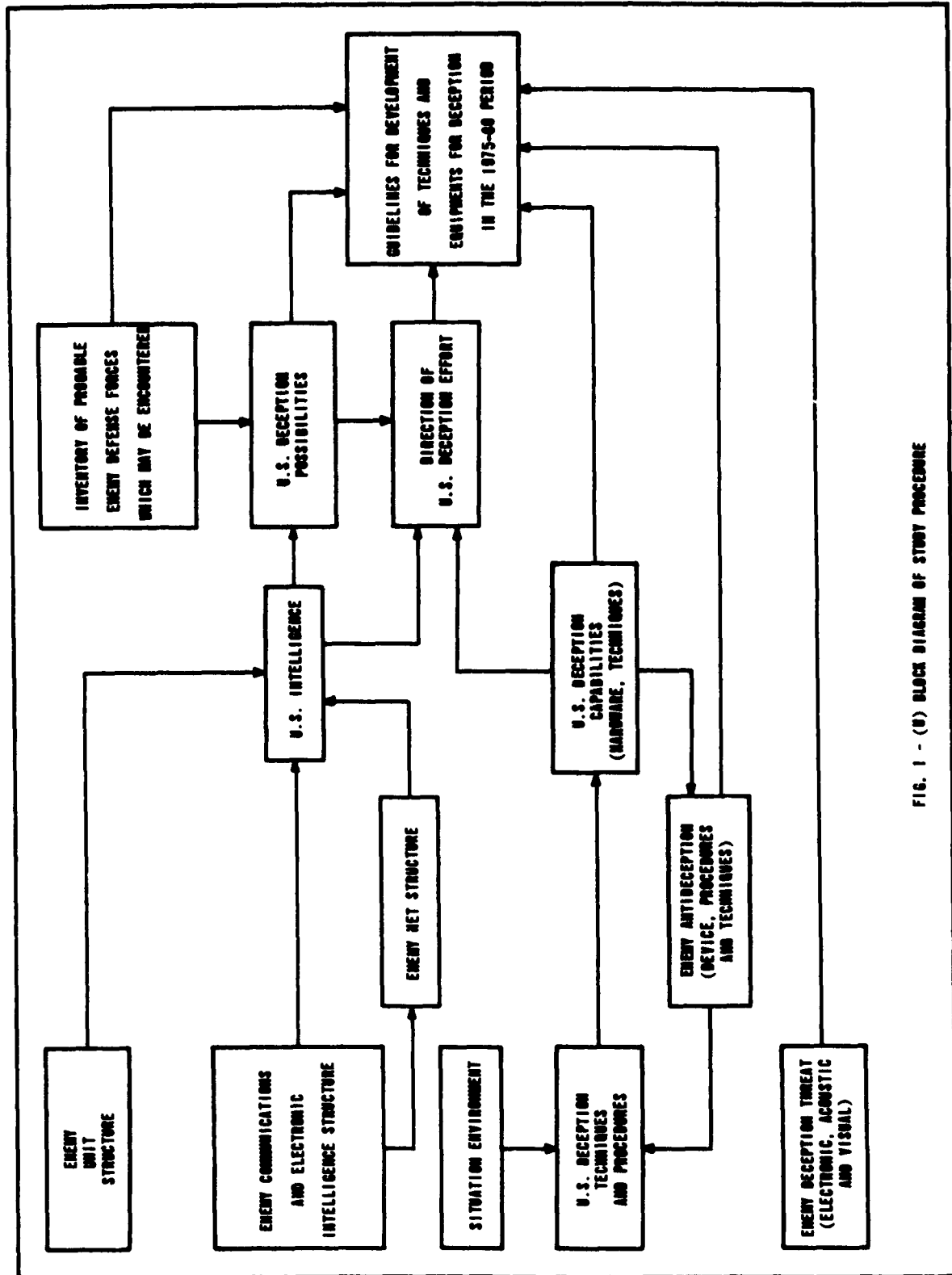


FIG. 1 - (U) BLOCK DIAGRAM OF STUDY PROCEDURE

II. THE 1975-1980 AMPHIBIOUS ASSAULT

Before the role of communications deception in amphibious assault operations of the 1975-1980 time period can be analyzed, the important parameters of the problem must be defined. For convenience of discussion, these parameters may be classified in three broad categories: (1) the U. S. amphibious assault philosophy, forces, and capabilities, (2) the enemy defense philosophy, forces, and capabilities, and (3) the state of communications technology for the 1975-1980 period. Each of these general categories is discussed in the following sections.

A. U. S. FORCES AND OPERATIONS

1. The U. S. Philosophy of Amphibious Assault

Amphibious assault operations in the 1975-1980 time period will be conducted on the same general principles as the "traditional" World War II operations. Yet even though the principles and objectives of these operations will remain essentially unchanged, the operational techniques will be considerably different from the massive operations of the World War II era.

The basic principle of the amphibious assault will remain unchanged: to establish an overwhelming preponderance of strength in the landing area so that the U. S. beachhead and subsequent breakout can be achieved quickly and effectively. U. S. control of the air and the sea will be required to minimize the attrition of the assault forces and to prevent enemy reinforcement of the defenses in the landing area.

In the 1975-1980 time period several factors will necessitate changes from the traditional World War II type of operation, which reached its fullest refinement in the invasion of Okinawa. First, the advent of nuclear weapons means that amphibious assaults against nations possessing these weapons, or even nations allied with nuclear powers, might be subjected to nuclear counterattack. Under certain conditions the nuclear threat might be eliminated -- for example, if an effective nuclear weapons control agreement could be established and enforced. At the present time, however, the chances for elimination of the nuclear threat appear to be dim, and the United States must be prepared for amphibious warfare in the face of this threat. For even if the enemy long-range missiles and bombers were destroyed prior to the

assault, a real threat would still exist in the form of nuclear artillery, short-range missiles, mines, and torpedoes. The U. S. assault forces would therefore have to be dispersed to minimize their vulnerability to nuclear attack. The type of operation used at Okinawa could be mounted in the future only where there is no possibility of nuclear counterattack. And the requirement for dispersal includes not only the landing area, but also the staging areas for the assault operation.

Second, the development of new types of vehicles means that amphibious assault operations in the future can be much more flexible and effective than in the past. Helicopters, for example, have dramatically increased the mobility and versatility of military units; thus the technique of vertical envelopment will be much more prominent in 1975-1980 operations than in World War II. The reconnaissance, intelligence, communications, weapons, command/control, and other systems associated with these vehicles will also be dramatically advanced in 1975-1980 as compared to World War II technology.

Finally, the U. S. must be prepared to face a wide range of situations in which amphibious assault operations might be required. These situations range from an all-out nuclear war to limited and guerilla war situations. Because of this wide range of military requirements, the U. S. amphibious warfare doctrine must remain rather general, and each operation will have to be tailored to the specific military situation.

2. New Capabilities for the 1975-1980 Period

As we have shown in the previous discussion, the basic principles and objectives of amphibious assault will remain unchanged for the 1975-1980 time period. The techniques for attaining these objectives, however, will change somewhat because of advancements in technology. The present discussion, therefore, will be concerned primarily with those aspects in which the 1975-1980 technology will introduce changes in the capabilities of U. S. amphibious assault forces for that period.

The 1975-1980 amphibious assault force will differ most radically from the "traditional" World War II force in its use of airpower. Whereas the World War II force relied on airpower primarily for softening up the landing areas and for close support of the landing operations, the 1975-1980 forces will

make extensive use of helicopters (and perhaps VTOL aircraft) in landing the assault forces themselves. The weakest link in the traditional operation was always the initial landing, in which small, highly vulnerable boats had to be loaded (often in rough water) with men and equipment, form up, and then move in slowly against the concentrated fire of everything which the enemy had left along the beaches. This problem can now be alleviated through the use of helicopters which, although vulnerable also, are much faster and more maneuverable and which could land the assault forces miles inland, if required. These helicopters will be capable of operating from the new amphibious assault ships and the new amphibious transport docks, as well as from a large number of other fleet types. By 1975 helicopters will have been developed which will carry anything but the very heaviest military material.

Nevertheless, it will still be more practical in 1975 to land many components of the assault forces, and especially their heavy equipment, over the beaches. But the use of small landing craft will be minimized. The 1975-1980 amphibious forces will use LST's to approach the beach wherever possible. This would minimize the delay in reaching the beach, exposure to enemy fire, seasickness, command and control problems, etc. Furthermore, within five minutes after beaching the LST can discharge 17 LVT's (Landing Vehicle, Tracked) with their complement of 350 to 600 personnel and a combat load of supplies. And the fact that the LVT is amphibious is an advantage in case the LST should run aground or be otherwise disabled before reaching the intended landing area. Other new Naval vehicles, such as the hydrofoil and hydroskimmer, are now under development and may be in operational use by 1975.

In general, then, the amphibious assault forces of the 1975-1980 era will possess far greater speed, versatility, and cargo capacity than traditional forces of comparable size of the World War II era. The 1975 forces will possess far greater fire power, better intelligence information, and more effective communications and command/control systems. Above all, they will possess a capability for vertical envelopment which will be much stronger than the paratroop capability of World War II. Yet even though these changes will revolutionize the techniques of amphibious warfare, they will not change its fundamental principle: to confront the enemy at the chosen beach with overwhelming U. S. land, air, and sea superiority.

3. Major Phases of Amphibious Assault Operations

A full-scale amphibious assault is a complex operation which requires the coordination and control of a wide variety of military units and activities. Each of these units and activities has certain communications requirements of its own, in addition to the requirements imposed by the operation as a whole. These communications requirements and their implications for enemy surveillance and U.S. communications deception operations are discussed in general terms in the following subsections.

a. Planning

Soon after a decision to conduct an amphibious assault has been made, an intense effort is directed toward planning and coordinating the various tasks of the operation. A major amphibious assault is of such magnitude that even during the planning phase there arises a considerable increase in the communications traffic of all the participating headquarters. This increase can be attributed to several factors. Unit training programs are accelerated in an effort to meet training requirements and qualify all personnel in their specialty. Field exercises and maneuvers increase in size and frequency. Logistical channels show an increase in activity as units must be brought up to 100 per cent strength with respect to supplies and equipment. Current intelligence information and reports from surveillance of the proposed objective area must be made available on a continuous basis to the commanders and staffs who are planning the operation. Communications play a major role in directing and coordinating the functions of these activities. Therefore, any increase in these activities establishes a corresponding need for more communications.

Superimposed on this communications need is the requirement for security as well as reliability. Often the participating headquarters will be separated by considerable distances thus requiring elaborate networks in order to maintain reliability. The problem of security is present in every communications transmission, the degree of security required being a function of the transmission value.

The mere fact that a rise in communications traffic has occurred can be of considerable value to the enemy. It certainly is one of the many indicators that he will be looking for. Hence, concealing this fact would give the enemy less information upon which to base his decisions and would be highly desirable from the U.S. point of view.

It can be expected that enemy espionage activities will be carried on in the vicinity of U. S. troop installations and training areas as well as other strategic areas under U. S. control. It is therefore anticipated that a major threat to an amphibious operation during its planning stage arises if enemy agents are able to gain important information by monitoring U. S. activities through interception of communications. If espionage activities of this nature are successful the enemy obtains a considerable time advantage in preparing his counter operation. Hence, there exists a need to deny information of this sort to the enemy or deceive him as to the information content.

b. Embarkation

This phase requires a large measure of coordinated effort among the various units of both the landing and Naval forces, as well as between the parallel echelons of these forces. Before embarkation can begin, plans must be provided for adequate communications between the Naval elements and the forces to be embarked. The landing force commander is normally assigned the responsibility of planning for and obtaining the communications in the embarkation area. This includes coordination of permanent and temporary facilities, military or civilian, with both the landing and Naval forces in order to insure that the organic and inorganic equipment of the various units is properly transported and loaded on the correct shipping. It further insures that no bottlenecks develop in the logistical lines over which supplies are being transported from storage areas to embarkation sites. The actual embarkation of troops and personal gear requires special communications planning in order to maintain adequate control over all loading activities. The fact that embarkation in future operations will take place at a number of ports adds considerably to the already existing communications requirements.

A large majority of these special communications activities are dissolved upon completion of embarkation. Hence communications traffic in the various areas of embarkation exhibits a sharp decrease. This fluctuation of communication traffic is quite readily detectable. Even without examination of message content, the signal externals and communication fluctuation patterns present to the enemy some useful information concerning the activities taking place.

As ships depart the embarkation area, a noticeable change again occurs as communications traffic is further reduced. The staging points which just recently were extremely active with troop movements, logistical functions, and embarkation procedures now stand nearly silent. The absence of communications activity as recognized by enemy sensors has many implications, one of which is that a large number of troops have evacuated the area. Denying the enemy this sort of information would certainly enhance the chances of success in achieving surprise and this in turn would reduce the cost of the operation.

c. Rehearsal

If time permits and security can be maintained, a rehearsal of the assault operation affords the planners and coordinators a splendid opportunity to correct those operational deficiencies which were previously not apparent, but which might otherwise seriously affect the operation.

Of particular importance is an evaluation of the communication applications in controlling and coordinating the exercise. In order to obtain the best possible assault phase coordination, all areas of communications activity which are required for the actual operation should be tested during the rehearsal. This, however, presents several problems. The enemy is given an opportunity to detect rehearsal operations. This results in focusing his immediate attention on the rehearsal activities in an effort to learn more about them. Communication equipment characteristics as well as operating procedures are indicators that permit the enemy to hypothesize concerning which types of units are participating, what equipments are involved, and what activities are being performed. The more time spent in rehearsal, the more the enemy can determine from his intelligence activities. Therefore, any gain derived from excessive rehearsal activities must be weighed against the probable disclosure of intentions to the enemy.

Because of the threat of a nuclear strike, concentration of forces can be safely effected only for short periods of time. It seems advantageous, therefore, to conduct rehearsal operations with some degree of dispersion. One method that can be employed is to hold separate rehearsals for the various elements of the amphibious force whose mission requirements are closely related. This, however, is not quite as effective as joint rehearsals and does not test all areas of coordination and control. The degree to which security can be maintained

in the rehearsal area will dictate whether rehearsals are conducted jointly or separately. It may be that it is not feasible to hold any rehearsal activities whatever. This may occur not only for lack of secure rehearsal areas, but also because of lack of time. In any event, the conduct of rehearsals does require a variety of deceptive measures to prevent disclosure to the enemy of the planned assault.

d. Movement To the Objective

This phase of the operation includes those activities of the main body of the amphibious assault forces from the time embarkation is completed until just prior to the assault itself. It is true that rehearsals are sometimes conducted during movement, but this will not be considered here as it has already been discussed.

It is very unlikely that a force of Naval vessels maneuvering in international waters will go undetected by the enemy. The enemy's information gathering system will surely contain complex airborne as well as satellite-borne surveillance equipment employing multiple-sensor techniques and possessing the capability to detect and monitor the activities of all major Naval force operations.

It may be possible, however, to avoid detection for short periods of time and under certain weather conditions. Efforts directed toward developing techniques for stimulating the atmosphere so as to cause fog, rain, and the like seem to be our best hope of avoiding detection by high resolution photo and infrared sensors.

Enemy detection of an amphibious force, although important, is not sufficient information upon which to base a decision concerning defensive actions to be taken. Although a certain measure of strategic surprise may be lost, tactical surprise can still be maintained as long as the enemy is unsure of the task force intention, the timing of the assault, the approaches to the objective, the landing beaches, and the composition of the assault force.

Since the possibility always exists that what the enemy has detected is merely a deceptive activity, the commitment of his resources for counter action, without supporting information about the apparent threat might prove disastrous.

Hence, although detection is likely to occur and strategic surprise may be lost, tactical surprise can be exploited as long as the tactical aspects of the operation are hidden, concealed, or otherwise denied to the enemy.

In future operations, the practice of convoy movement will be forced to give way to more dispersed, self-protecting, smaller movement groups in order to avoid the mass destruction potential of the enemy as well as to add to the difficulty of detection. This, however, requires even more coordination than was previously needed for convoy movements. The usual restriction of radio communications and maximum use of helicopter messenger, and visual communications may result in insufficient coordination between various task groups. Hence other communication schemes will be required. Use of the optical spectrum offers one possible solution to this problem. This is considered in more detail in a later section. In any event, the need for coordination exists and to be effected properly requires secure communications. If radio communications are used, denial to the enemy of the electromagnetic emissions is mandatory.

Reliability is essential in the communications employed for no mistake can be tolerated if, because of bad weather or enemy action, the planned assault has been postponed or alternate plans have been put into effect.

e. Preassault Operations

Operations of all forces in the objective area prior to the arrival of the main body are to be considered preassault operations. Although preassault activities are generally not treated as a separate phase of the amphibious assault, they appear to be of great tactical importance and a large measure of tactical surprise may be lost if proper deception is not employed in the conduct of such activities. The proper conduct of deceptive activities constitutes the chief feature in achieving tactical surprise. Therefore, the extent to which these preassault activities may be utilized to achieve maximum effectiveness in the overall operation is dependent upon the relative interplay between the anticipated tactical advantages and the possibility of disclosing both particular and general intentions to the enemy.

Elements of advance force operations may thus consist of many deceptive and tactical activities, the particular combination of which is dependent upon the specific objectives of the assault operation. The actions of an advance force

as well as other preassault elements may thus be employed in a variety of combinations to achieve the desired results. The following preassault activities require deceptive efforts not only to enhance their successful completion, but also to avoid disclosure of assault force intentions.

1. The destruction of general or specific enemy defenses and fortifications situated ashore.
2. The preparation of sea areas for reception of assault forces.
3. The preparation of beaches and approaches.
4. The aerial surveillance and ground reconnaissance of the various beach heads.
5. The isolation of the objective area.
6. The maintenance of surface, subsurface, and air superiority.
7. The conduct of harassment and other techniques of psychological warfare.
8. The collection of information concerning enemy operations.

f. Assault

The assault phase begins when the elements of the main body of the amphibious task force arrive in assigned positions in the objective area and terminates with the accomplishment of the amphibious task force mission. It includes:

1. The coordinated ship-to-shore movement of the landing force.
2. Landing of paratrooper, helicopter-borne and water-borne assault forces at their respective drop zones, landing zones, and beaches.
3. Inland operations by all units to secure the beach head.
4. Provision of logistic, air, and naval gunfire support of the attack by the naval forces throughout the assault.
5. Landing of back-up force and reserve force elements to conduct such operations as may be necessary to accomplish the amphibious force mission.

Admittedly, all such activities will be scheduled in the planning phase of the operation. Nevertheless, their execution will require extensive measures of coordination and control. Hence, in contrast to the relatively little detectable communications traffic during the preceding phase, the assault requires extensive communications to insure timely and coordinated execution of the landing force mission.

By the time the assault phase is to begin, it is almost certain that an alert enemy will have had sufficient time and information about the amphibious operation that he will commence fortifying those defensive positions which lie in the general direction of the amphibious force movement. The fact that an amphibious landing is imminent will be quite apparent; however, if deception efforts have been successful thus far, the enemy will still be at a tactical disadvantage. Not only will he be in doubt as to the exact timing and location of the assault, but the amount of time available to him to move reserve forces and equipment to the probable area of the assault will be sharply limited. The high speed approach to the beach via surface and air vehicles from 30 nautical miles or more from shore will place the initial wave of assault forces on the beach within an hour from the time the ship-to-shore movement begins.

Deceptive efforts during this phase appear to be most promising when employed to increase the reaction time of the enemy in the making of decisions and the movement of his reserve forces. Realistic employment of feints, raids, demonstrations, and diversionary attacks, as well as those deception techniques to degrade the enemy estimates of the timing of the assault and the strength of the assault forces provides a good means of accomplishing this end.

Since time is of the essence, every minute of hesitation on the part of the enemy provides the assaulting forces with greater tactical advantage. The fewer the enemy forces opposing the initial assault wave, the swifter the beachhead can be established. Hence, not only will the initial assaulting forces suffer fewer casualties, but successive assault waves will hit the beach in the face of continuously diminishing opposition.

B. ENEMY FORCES

A U.S. amphibious warfare system for the interval 1975-1980 must be prepared to meet each of a wide range of defenses. The established coastal defenses of the Soviet homeland are only one extreme. Hasty defenses on the flanks of Soviet forces in a theater of operations and the more primitive defenses of less developed nations must also be taken into account.

Not all of the possibilities can be considered explicitly in this study. Yet most of these defenses will have been established according to Soviet military doctrine or some derivative of it, and most of them will employ Soviet materiel or materiel of Soviet design. It seems reasonable, then, to use Soviet forces, their organization, equipment, techniques and doctrine as a model in estimating the enemy forces opposing the amphibious warfare system.

Except for special cases, it can be assumed that the preponderance of force lies with the defense against an amphibious operation but that the attacking force must have local superiority if the attack is to be successful. Naval and air supremacy during the debarkation and assault are also assumed necessary for success. Consequently, surprise is a decisive factor and this analysis of the defending force is concerned principally with security against surprise measured in terms of the time required to reinforce the defense at the assault point.

"Security," in this sense, involves:

- natural obstacles to an assault landing
- disposition of defending forces along the defended coast
- disposition of mobile reserve forces
- displacement times and column speeds
- disposition of air elements
- command organization of the defense
- intelligence collection means
- intelligence processing methods and decision processes
- communications system.

1. The Soviet Philosophy of Defense Against Amphibious Assaults

The Soviets possess few coastal areas which would be seriously threatened by large-scale surprise amphibious landings during time of war. Consequently, they have not displayed great concern with the problem of defense against such landings. However, Soviet coastlines do provide numerous target areas which, at suitable times of the year, might be objectives for amphibious landings of regimental and divisional scope, particularly in conjunction with or support of land operations. The doctrine which they have developed for defense against amphibious landings is designed to cope primarily with such operations.

The Soviet anti-amphibious doctrine leans heavily on German World War II experience and study of U.S. amphibious techniques. A flexible anti-amphibious doctrine has evolved which can be modified to fit local conditions of terrain, climate, and physical facilities. The more important Soviet coastal areas have been prepared for defense to some extent. Units stationed in the Murmansk-Archangelsk area in the north, along the Baltic and Black Seas, in Kamchatka, and elsewhere along the coasts of Eastern Siberia have been earmarked for coastal defense and trained in its techniques.

The basic Soviet defense against amphibious landings contemplates a well prepared strongpoint defense in critical areas forward along coastlines backed by strong mobile forces, predominantly tank units. The latter are to be held in assembly areas from which they can be moved quickly to counter any enemy threat to break out of the developing beachheads. Naval and air patrols, coast watchers, radar, and other means will be used to detect any enemy buildup and preparations for amphibious operations and initiation of his movements by water. Wide reliance will be placed on long-range agents located near potential amphibious staging areas and at points where naval operations can be kept under surveillance. On the assumption that most amphibious operations will be supported by airborne landings, close ground and air surveillance will be maintained over U.S. air bases in an effort to detect any preparations for airborne operations.

The main defensive effort will be aimed at destroying the amphibious elements during their debarking operations or while they are still on the beaches. Meanwhile, specially designated mobile antiairborne units in the rear will seek to pin down or neutralize any airborne assault units. As the pattern of the amphibious operation unfolds, particularly if there is success in forming a beachhead, some of the mobile reserve units will be brought forward into blocking positions. However, should the U.S. succeed in landing its armored units and breaking them out from the beachhead the main mobile reserve units will be committed as a counterattack force. Meanwhile, a steady buildup of naval and air strength, particularly submarines and attack aircraft, will seek to neutralize the naval and air support of the landing forces and isolate them from reinforcement or support.

A defense in which a typical Soviet motorized rifle division with supporting elements is responsible for up to 30 kilometers of coastline is favored where coastal landings could provide ready access into the interior, as along the Baltic and Black Sea coasts. Such a defense probably would involve a number of divisions under the direction of a Soviet Combined Arms Army, or it might involve several armies under the command of a military district or front. The mobile reserves for this type of defense would comprise the tank regiments of the divisions, the tank divisions of the armies, and possibly one or more tank armies. Each beach area on which landings might be made would be prepared defensively and the defenses continuously manned.

The defense as prepared would be based on the concept of battalion strongpoints located back on high ground away from the water's edge. Each such strongpoint would be from 2 to 4 kilometers wide and up to 3 kilometers deep. On extended beaches the strongpoints might be up to 1 kilometer apart so that the total zone of responsibility of a motorized rifle regiment might extend from 8 to 15 kilometers, depending on whether it is organized in one or two echelons. The two-echelon regiment with two battalions in the first echelon is normal. In this case the second-echelon battalion's positions start 1 or 2 kilometers behind those of the first-echelon battalions.

In general, the battalion strongpoints are situated so as to provide for frontal fire extending well out beyond the water's edge, interlocking and flanking fire with adjacent battalion or separate company strongpoints, and protection for coastal and field artillery. The strongpoints will be carefully prepared, including, if time permits, concrete, log, or sandbagged positions for the coastal and other

artillery, antitank guns, and automatic weapons. The beach areas in front of the strongpoints and the areas between them will be heavily sown with antitank and antipersonnel mines and will contain antitank ditches and other types of obstacles to the movement of tanks and other vehicles. Steel rail and other obstacles to the approach of landing craft will be emplaced to well out beyond the water's edge. Barbed wire will be used extensively in front of and throughout the strongpoints as an obstacle to foot movement. In addition, mines will be sown in specified areas within the strongpoints to slow up the assault forces in the event they succeed in overrunning the forward positions. The artillery emplaced within the strongpoints will be designed primarily for the delivery of flat trajectory fire against the ships offshore and, more importantly, the approaching landing craft. Heavy use will be made of mortars, rocket launchers, antitank weapons, and field artillery emplaced in the rear to provide a blanket of fire covering the beach all the way from the forward edge of the strongpoints out to the extent of the underwater obstacles.

A two-echelon division formation, involving the establishment of defense positions for a second-echelon regiment some 8 to 10 kilometers back from the coastline to cover likely avenues of approach, will be used when sufficient forces are available. In any case, areas between and behind the battalion strongpoints which do provide avenues for the movement of armor will be sown with mines and other obstacles, and all important junctions and armor bottlenecks will be covered by tank traps involving the fire of antitank weapons and assault guns. The division's mobile reserves, its tank regiment, will be held in an assembly area some 10 kilometers back from the coastline and convenient to routes by which it can move to attack penetrations anywhere along the front of the division. The tank division of the army's mobile reserve is held in assembly areas some 15 to 30 kilometers to the rear.

A wider-front defense would be used on coastlines which have few suitable beaches for landing operations and only limited opportunities for movement inland off the beaches. This is the type of defense which the Soviets might be expected to employ along the coastal areas of Eastern Siberia. In this type of defense the division would have a frontage of 45 kilometers or more. Only those landing areas which contain important amphibious objectives or promise access to such objectives would be prepared for defense. Most of these would be only lightly manned, the main body of defensive troops being held back for movement

to threatened areas as required. The wide sectors of coastline between those areas prepared for defense would be covered only by patrols or coastwatchers as protection against infiltration landings and commando raids.

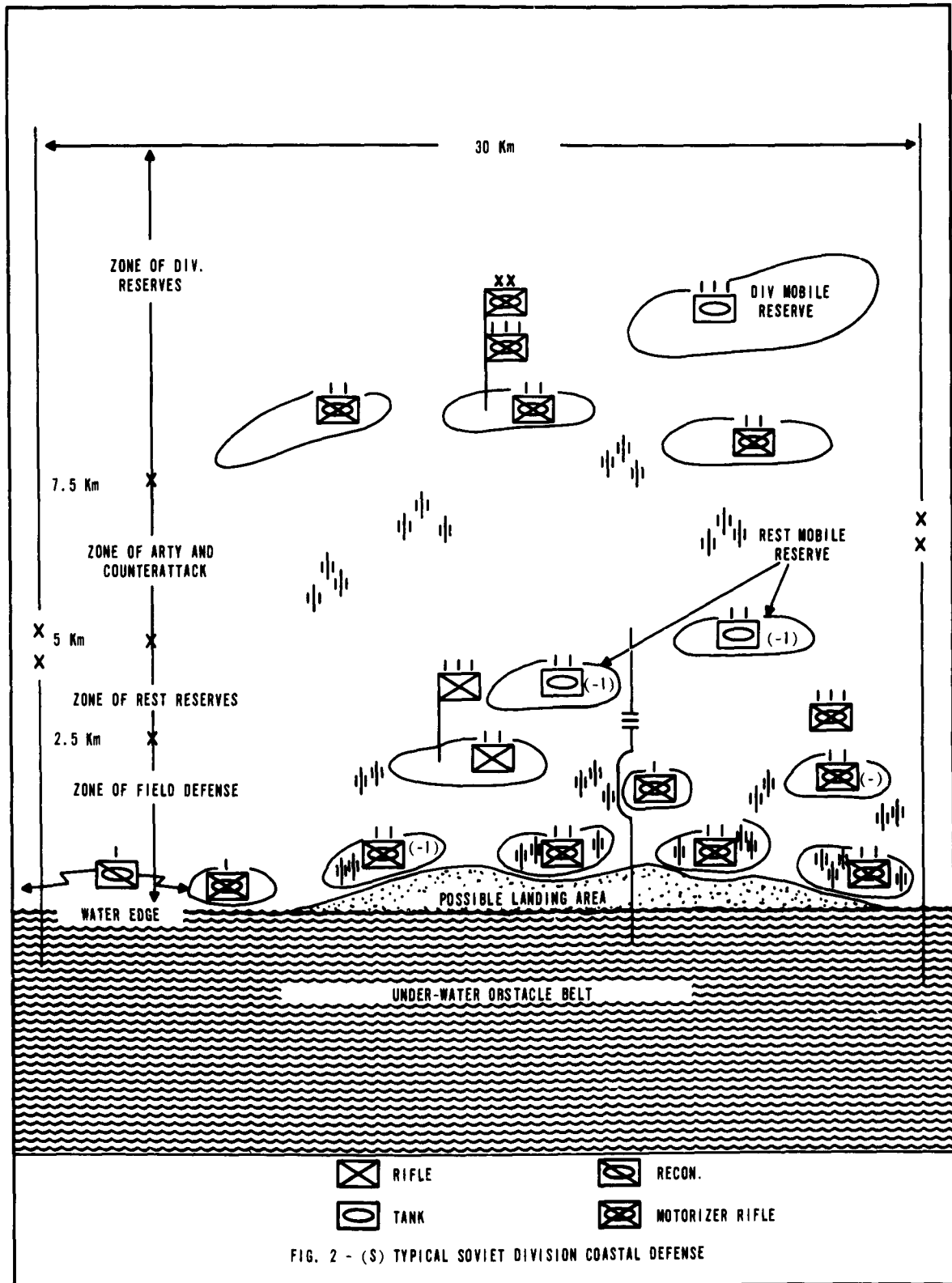
The Soviets consider the amphibious defense as starting at the moment firm indications have been received that the movement of ships for an impending amphibious operation is underway. At this time all available air and naval power will be brought to bear against the convoy in an effort to destroy it, cause it to disperse, or force it to turn back. This will also be the time of major effort to secure air superiority and to disrupt the U.S. plans for airborne assault, since the loss of air superiority would probably cause the U.S. to cancel the attack plans.

Should the assaulting forces succeed in reaching the point for debarkation of troops on amphibious craft or for other movement onto the beaches, they will be brought under the fire of coastal artillery. This also would be the time for maximum use of nuclear weapons if they are available. As the assault craft approach the beaches they would be subjected to heavier and heavier fire as more weapons are brought to bear. The actual arrival of U.S. troops onto the beaches is considered the critical time of the first phase of the defense. Every effort must be made to pin them down and prevent them from moving frontally against the strongpoints. In particular, they must be prevented from successfully landing their armored vehicles and moving them off the beach to areas where they can operate efficiently.

Recognizing that during this time the assaulting forces will be receiving naval fire support and that possibly only a portion of the intended defenses will be capable of direct action against the landed troops and, therefore, will not be able to neutralize them completely, the main defensive effort will be designed to channel the attacking forces into the areas between the forward strongpoints. Once the advance has carried them inland a short distance, it will then be possible to simultaneously bring them under fire on the rear and flanks from the forward strongpoints and frontally from the strongpoints of the second echelon. In addition, limited objective counterattacks supported by tanks may be mounted against threatening penetrations from the strongpoints themselves.

Should the U.S. buildup continue and a genuine breakout threat develop as a result of neutralization of the strongpoints and advance by U.S. armored elements into the rear of the coastal defenses, a series of counterattacks by

SECRET



SECRET

armored units of regimental and divisional size will be made with the objective of pinching off the armored spearheads, driving them back onto the beaches and permitting re-establishment of the strongpoints.

The Soviets realize (1) the futility of assuming that their defense will successfully defeat or neutralize every assault by a determined and skillful amphibious force and (2) the impossibility of adequately defending every possible amphibious landing point. Moreover, they assume that most amphibious operations of the future will be supported by nuclear strikes which can eliminate the possibility of coastal defense well before the first units are landed. Consequently, the Soviets will practice defense in depth as a means of insuring that successful amphibious landings will not develop into full-scale offensive operations. Armies and Fronts or military districts will retain substantial combined arms and tank units in deep reserve prepared to carry out mobile defense at any point. They believe that in view of the semilandlocked character of the Soviet mainland, there is little likelihood that any nation could successfully mount an amphibious operation that would not be detected in sufficient time for these back-up troops to be alerted and moved to preselected areas for containing the offensive.

2. Beachhead Reinforcement Capabilities

Present day Soviet infantry is able to march at 4-5 kph during the day and 3-4 kph at night. Soviet motorized and armored units are able to move over roads at 20-25 kph in the daytime and at 15-20 kph at night. Cross country movement reduces these figures by one half to two thirds.

By 1975, improvements in tracked vehicles may result in column speeds of 35-40 kph while developments in night driving equipment should reduce or eliminate the difference between day and night march rates. In a prepared amphibious defense, little time will be lost in cross country movement since the defending force will have had opportunity to lay tank trails and to rehearse the possible reinforcing movements.

Column lengths, on the other hand, are not expected to change much between now and 1975. Currently a motorized rifle division in march formation is 140 to 160 km long while a tank division has a column length of 130 to 150 km. If as many as four or five parallel routes are available, about one hour is required for a tank division to clear its assembly area or to take up combat positions from the march.

Using these estimates, the time required to reinforce front line units with mobile reserves is typically:

Reserve Echelon	Reinforcing Units	Distance	Time
Front	Tank Divisions	90 - 350 km	4 - 12 hr.
Army	Regiments of Tank Divisions	30 - 90 km	2 - 5 hr.
Division	Battalions of Tank Regiments	5 - 15 km	20 - 40 min.

3. Intelligence Collection Means

The forces defending against amphibious assaults may employ a wide variety of techniques for the collection of intelligence information concerning the assault forces. The enemy will attempt to employ these techniques throughout the assault operation, from the initial planning stages until the conclusion of the combat operations. Each of these techniques exploits some physical phenomenon, and most of them can be utilized with more than one kind of surveillance or reconnaissance platform. Passive sonar, for example, may be employed by shore stations, in aircraft which monitor sonobuoys, by helicopters or blimps, by surface ships, and by submarines. The ultimate effectiveness of the sensor system, therefore, is determined by the platform as well as by the sensor itself.

The following discussion of intelligence collection techniques has been organized according to the surveillance or reconnaissance platforms. At the request of the Contracting Officer, special attention has been devoted to the earth satellite as a vehicle for intelligence collection. Since extensive information is already available concerning most of the other platforms, those discussions are rather general.

a. Satellites and Space Vehicles

Earth satellites are now being used in various military and civilian applications: communications relay, navigational aids, scientific research, and surveillance and reconnaissance. Among the advantages of the satellite are its ability to cover areas to which other vehicles are denied access,

its high ground speed (and correspondingly high search rate), and its large field of view. Its most important disadvantages are its lack of versatility and its restricted payload. Both of these disadvantages are becoming less serious as more "sophisticated" circuitry and larger boosters are developed. A disadvantage which will become more serious, however, is the satellite's vulnerability to countermeasures.

Because of their high search rates and sweep widths, satellites appear attractive for ocean-wide surveillance systems. Their high altitudes and their power limitations, however, place constraints on their detection capabilities. By the 1975-1980 time period, however, a wide variety of sensors could be considered for use in satellites.

If the satellite or space vehicle were manned, the human observer would be very effective in detecting amphibious assault forces on the surface of the sea below in conditions of good visibility. The wakes of surface ships are visible even at night at very high altitudes, especially when the water contains phosphorescent organisms. The human observer is especially useful in making quick evaluations of targets which have been picked up by other means. Certainly in any full-scale war during the 1975-1980 period both sides can be expected to use manned space platforms for surveillance.

A variety of passive optical systems can be used in satellites. These systems can be built for operation in the visible, infrared, or ultraviolet portions of the electromagnetic spectrum, and may be instrumented for real-time or photographic readout. Television scanners, for example, are feasible for use in unmanned satellites. The video signals can be telemetered directly to the ground, relayed to another satellite, or stored for later readout over a command/control station. Infrared scanning systems for the 1975-1980 period will be capable of angular resolution of .25 milliradians and temperature resolution (limited by atmospheric variations) of .0025°C. This is more than adequate for the detection of surface ships at sea and to discriminate between nuclear and conventional power plants. Shallow and snorkeling submarines can also be detected with passive infrared systems.

Active optical systems could certainly be employed in satellites and space vehicles by 1975. Lasers, for example, are inherently capable of extremely accurate range resolution and could be used in situations where the ambient light

level is too low for passive systems. Present lasers are inefficient and require too much power to be suitable for practical use in space vehicles. By 1975, however, laser efficiency and the power available in space vehicles will have improved dramatically, so that lasers will probably be practical for ocean surveillance from a satellite.

Because of the shorter wavelengths involved, the visible light systems afford better resolution than the infrared systems. Both types, however, are limited by atmospheric turbulence, the size of their optical apertures, and most important, by moisture in the atmosphere. Neither infrared nor visible light systems can penetrate heavy cloud cover.

Surveillance systems operating at radio frequencies are also feasible for use in satellites and space vehicles. Passive techniques can be used to intercept radar and communications transmissions originating from surface ships and other elements of the amphibious assault force. Even with the current state of the art, automatic recognition of known signals is possible. Radars can be automatically identified by function (e. g., search, fire control) and in some cases by type (SPS-No.). Various communication modulation types (e. g., FM, FSK) are also easily recognizable, although automatic recognition of the semantic content of communication signals is not feasible. These passive intercept techniques, of course, would be effective only if the amphibious assault force broke radio silence. Location accuracy with these techniques is about 1 milliradian.

The use of radar for ocean surveillance in satellites and spacecraft in 1975 will be feasible. Pulse compression radars have already been developed which can discriminate one foot in range by selected range increments, under laboratory conditions. The limitations on the effectiveness of radar systems will be the power which is available in the spacecraft and the identification of the target in the sea return. The latter problem is most critical for those targets which lie directly beneath the satellite's track. Radar effectiveness against surface ships deteriorates somewhat in heavy weather. And radar, of course, is vulnerable to jamming by the enemy.

The enemy could also use satellites and spacecraft in conjunction with sensors on the surface of the earth to provide warning against U. S. naval operations. Satellites are excellent relay stations for communication

transmissions and could be used, for example, to relay initial contact messages from enemy submarines to their operational commanders. Highly directional transmissions to satellites from strategically placed sonobuoys or from spies at U. S. naval activities would also be possible with much less risk of discovery than in conventional surface-to-surface transmissions.

Methods to intercept, inspect, and neutralize or destroy enemy satellites and spacecraft are now being developed. By 1975 these methods should be operational, and supremacy in space may become as necessary to the success of amphibious operations as supremacy in the air and on the sea. At any rate, it seems obvious that no movement of surface ships can be considered secure if it has been observed by enemy satellites or space vehicles, and that the destruction of such vehicles will be a prerequisite to any landing in which there is to be any element of surprise.

b. Aircraft

Overflight by aircraft is probably the most effective way to collect intelligence on a naval task force. It is also extremely dangerous. But there is little doubt that by 1975 the Soviets could develop aircraft capable of attaining extremely high speeds and altitudes. Such aircraft, because of their maneuverability, would be less vulnerable than satellites in fixed orbits. If they were equipped with telemetry links, these aircraft could probably transmit at least some valuable intelligence information even if they were successfully intercepted. Furthermore, an attempted overflight by the enemy could force the Navy to activate radar, guidance, and communications transmitters which would otherwise have remained silent. This, in turn, would provide extensive information to enemy signal intelligence analysts, as well as reveal the position of the task force to enemy DF stations.

Enemy aircraft could be equipped with any of the sensors mentioned in the discussion of satellites and spacecraft. While high-altitude, high-speed aircraft would attempt overflights or at least provoke the task force into defensive action, other high-speed aircraft would attempt low-altitude penetrations. When the location of the task force becomes accurately known, penetration beneath the lower limit of radar coverage may be the most effective technique for reconnaissance or attack. Patrol aircraft would be used for routine ASW searches and the monitoring of sonobuoys. These aircraft would be

equipped with magnetic anomaly detectors and the equipment required for recording and analysis of the sonobuoy outputs.

c. Surface Ships

Enemy surface ships can be expected to patrol the offshore waters to defend against submarines and to warn against intruding low-level aircraft. They might also be used in an attempt to locate and destroy Polaris and other submarines, although this would be feasible only in ice-free waters. At any rate, it is unlikely that enemy surface ships would make contact with an amphibious assault force, since air and sea superiority would be established in the area before the arrival of the assault force itself. Enemy surface ships might intercept radar or communications transmissions from the assault force, however, and would relay this contact information ashore. These ships might also make radar contact with aircraft of the assault force and in rare cases with ships of the screen.

d. Submarines

Enemy submarines are unquestionably regarded as the first line of defense against U. S. naval striking forces. These submarines would be responsible for reporting initial contact with the assault force, for collecting intelligence on it, for tracking it, and for attacking it as the opportunity arose. These submarines would operate only their passive sensors in their initial intelligence collection so that they would not alarm the assault force and provoke a fatal counterattack.

The passive sensors on these submarines would include radio intercept equipment, hydrophones, and periscopes. Upon first contact with the task force, the submarine would probably seek the best depth to avoid detection by the surface ship sonars and would track the task force with passive listening gear. Turn counting and analysis of machinery and other noises might be adequate for the submarine commander to classify the task force as an amphibious assault force. If this were the initial contact, he would then probably attempt to clear the area so that he could flash the contact message to his operational commander.

If the submarine commander knew that contact had already been made, or if he felt that he needed more information, he might risk a

periscope photograph of the task force. Or he could shadow the task force, analyzing their communications and radar transmissions, if any, and computing their course. He would probably not risk a radar or sonar transmission until he needed an accurate target range during the last phase of his attack.

The major problem in surveillance and reconnaissance by submarines is the transmission of the intelligence data. One technique which will certainly be feasible by 1975 is transmission, at a very high frequency and with an extremely directional antenna, directly from the submarine to an earth satellite, which would then relay the information. Another possibility is the recording of the data for retransmission from a buoy or balloon after the submarine has cleared the area. The submarine can transmit to an aircraft, of course, if the submarine is operating in an area of air superiority; in an amphibious assault, however, the assault forces must have air superiority.

e. Shore Stations

Shore based surveillance systems of several types can be expected to be employed in the defense against amphibious assaults. Although radar has an excellent range capability, its effectiveness against surface ships is limited by the curvature of the earth. Although there is some bending of the radar beams, this phenomenon does not permit echo ranging against surface ships which are very far below the visible horizon. HF "radars" have been developed for the detection of ion trails by ionospheric "bounce" techniques, but these are not effective against surface ships.

Radio intercept and direction finding stations are especially suitable for shore installations. The most accurate DF systems require a large amount of space for the installation of antennas and a considerable amount of signal intercept and processing equipment. Because the restrictions on size, weight, reliability, maintainability, and personnel are much less stringent at shore stations than aboard ship or in aircraft or space vehicles, the shore based intercept systems can achieve much higher performance, and often collect much more intelligence, than other systems. Unusual propagation anomalies, which are not yet fully understood, can extend intercept range far beyond what might normally be expected. Therefore, the amphibious assault force of the 1975-1980 period will have to operate under the assumption that the enemy could intercept any and all radar and communications transmissions, and some emission control plan will have to be implemented for the operation.

Extremely sensitive passive acoustic detection techniques are feasible where the hydrophone and signal processing equipment is not limited in size and weight. When large hydrophones can be installed in an optimum position a few miles offshore and coupled to extensive signal processing equipment ashore, detection ranges of several hundred miles can be achieved against surface ships. Of course, the amphibious assault force would attempt to destroy such installations before the assault if their existence were known. And because of the expense of such arrays, their number would be likely to be extremely limited. Installations would probably be restricted to critical points along the Soviet coast. Analysis of the output of such sensors can yield extensive information concerning the numbers and types of ships in a task force. Because some types of ships are used almost exclusively for assault operations, it is quite likely that the enemy could deduce the type of operation from this analysis alone.

Shore stations could also serve as monitoring stations for off-shore detection equipment of other types. Remote, fairly compact sonobuoys, for example, could be monitored by such stations. And magnetic anomaly detectors could also be used either separately or in conjunction with acoustic detectors to enhance the reliability of warnings from such remote installations. Equipment for the detection of sound in air might be used to detect the lowering of boats or the offloading of cargo, although such techniques have rather short range relative to the ranges of other detection techniques. Finally, shore stations would be used for visual observation of the offshore waters and for security patrols of the coastline to guard against the landing of covert forces.

f. Covert Techniques and Prisoner Interrogation

The enemy can be expected to use every covert technique at his disposal to discover the objectives, strength, and operational schedules of the amphibious assault force. These include all of the standard espionage techniques: spying on U. S. naval activities, acquisition of information from naval and civilian personnel, planting of agents in sensitive positions within military and governmental organizations, etc. The major difficulty confronting the enemy in this type of activity, once the espionage is successful, is the transmission of the intelligence information to the enemy intelligence activities in time for it to be of use.

Large-scale amphibious assaults must usually be preceded by a certain amount of reconnaissance and advance preparation of the landing areas by aerial reconnaissance, intelligence specialists, underwater demolition teams, etc. The capture and interrogation of such personnel by the enemy is a possibility. Although these personnel will have limited knowledge of the impending assault operation as a whole, the enemy may still deduce a great deal just from their equipment and a cursory knowledge of their mission. The mere fact that this type of activity has increased in a certain area would alert the enemy to the possibility of an invasion.

4. Intelligence Processing Considerations

Collection of intelligence data concerning the amphibious assault forces is only the first step in the defense against the assault. The data must be transformed into meaningful intelligence information, evaluated, transmitted to the appropriate command echelon, integrated into the total intelligence picture, and then evaluated once again before being used as the basis for tactical and strategic decisions.

5. If the amphibious operation involves preparation by small parties landed covertly or by frogmen prior to the assault, capture of prisoners and their interrogation is always a possibility. While these individuals need know nothing of the overall operation, it must be assumed that their individual missions will become known to the defense.

Crucial to the effectiveness of collected intelligence information is the time required in bringing it to bear on the situation. Prior to the assault phase, the defense is normally conducted at army level which is the highest tactical level of command. The decisions to be made include:

- a. Alerting emplaced and reserve defense forces.
- b. Committing air and missile forces in attack on the amphibious force at sea.
- c. Committing reserve units to march routes and/or to forward assembly areas.
- d. Lateral displacement of defense forces from coastal positions.
- e. Committing supplies and ammunition to convoy routes or to forward dumps.
- f. Committing reserve units to combat positions.

These decisions must be based upon the following elements of information about the attacking force.

- a. Its strength and composition in terms of
 - (1) Its capability to reduce the defenses by air, missile and naval gunfire.
 - (2) Its capability to interdict and isolate a sector of the coast.
 - (3) Its capability to make one or more amphibious assault landings.
 - (4) Its capability to make one or more airborne assault landings.
 - (5) Its capability for defending itself against air and missile attack.

- b. Its disposition in terms of the time required to concentrate and realize a specific threat or combination of threats at specific points.
- c. Its degree of commitment to an apparent course of action.
- d. The reliability of inferences about the attacking force.

Developments in the application of data processing, decision making, data transmission and automatic switching techniques which will occur over the next twelve to seventeen years will remove some of the most severe limitations of present day intelligence processing and dissemination methods. Some of the new modes of collection and the vastly increased tempo of offensive operations will require that present day methods of processing intelligence information be abandoned or at least supplemented.

The practice of evaluating intelligence information at a command level superior to both the collector and user and disseminating a finished product downward will, of course, continue but raw or semiprocessed data will also be disseminated directly to the headquarters of the users. High speed processing techniques, systematic dissemination, and flexible communications will make this possible without inundating each echelon with irrelevant information. Automatic data processing machinery at all echelons down to division will make interpretation of such data possible. It will become practical to provide pertinent intelligence information to all echelons down to army or division almost simultaneously.

A schematic of the routing of intelligence information to a Soviet Army commander conducting an amphibious defense is given in Figure 3. In the following paragraphs, the delays and time consuming actions which occur in the chain for each type of collection are discussed. Estimates of the magnitude of these delays are then summarized in Figure 4.

A multisensor satellite in low orbit may collect information at the rate of 10^7 bits/sec. or 10^{11} bits/orbit. Communication problems are such that the take must either be buffered and transmitted to certain stations on the ground while the satellite is in certain restricted segments of its orbit or considerable data reduction must be accomplished in the satellite. It is estimated that, rather

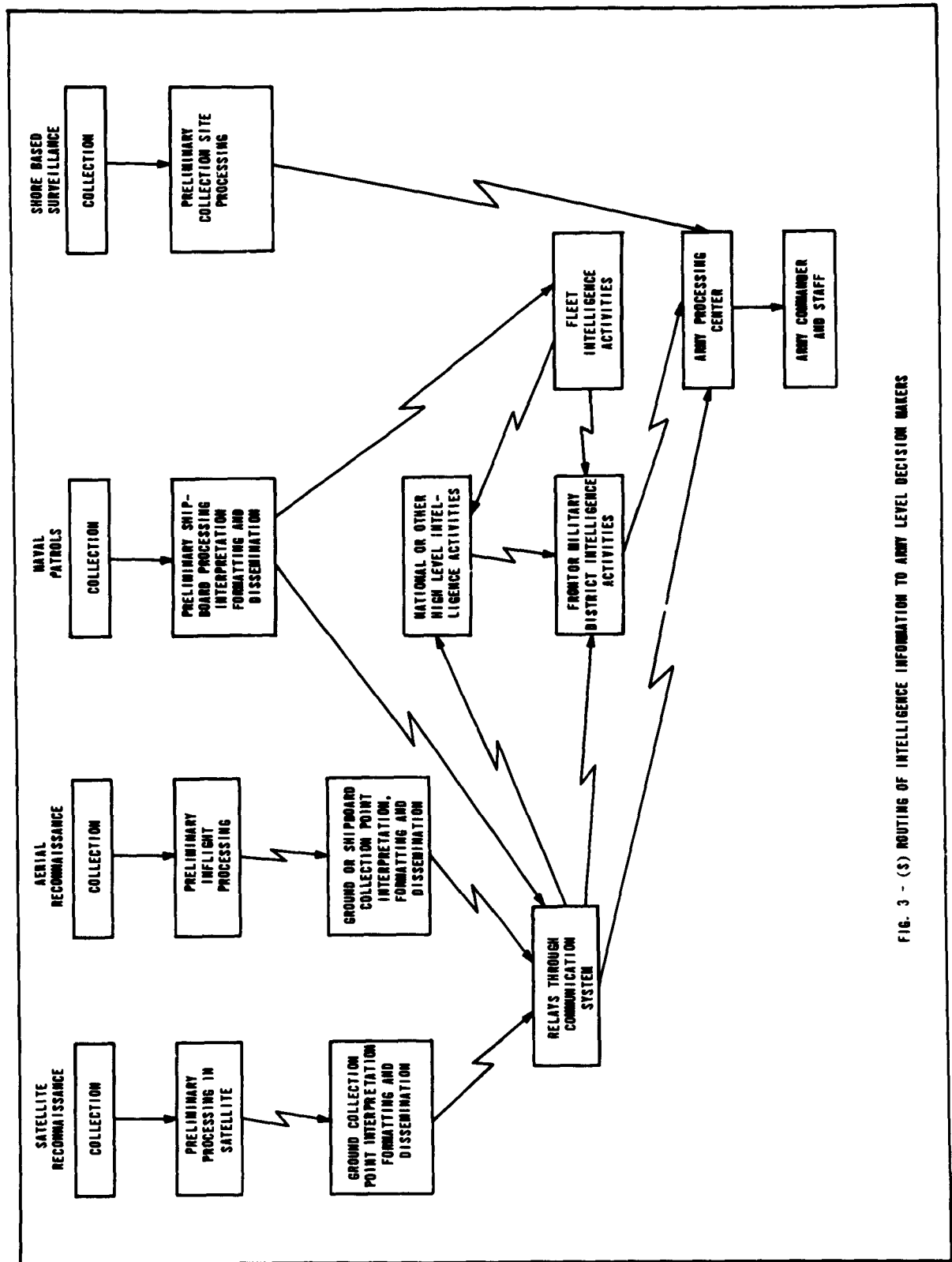


FIG. 3 - (S) ROUTING OF INTELLIGENCE INFORMATION TO ARMY LEVEL DECISION MAKERS

COLLECTION MEANS	SAMPLING RATE (SEE TEXT FOR DETAILS)	PRELIMINARY PROCESSING TIME	TRANSMISSION DELAYS TO GROUND OF SHIPBOARD COLLECTION POINT	INTERPRETING FOR BATTING AND DISSEMINATION TIME	DELAYS IN COMMUNICATIONS SYSTEM	ARMY PROCESS- ING TIME	TIME FOR DECISION AND START OF EXECUTION	REACTION TIME FROM CHANGE IN SITUATION TO START OF EXECUTION
SATELLITE RECONNAISSANCE	ONE COMPLETE SAMPLE EACH 90-120 MIN PER SATELLITE	1-3 MIN	5-10 MIN	1 MIN	1-20 MIN	1-3 MIN	1-5 MIN	10-162 MIN
AERIAL RECONNAISSANCE	ONE OR TWO COMPLETE SAMPLES PER SORTIE	1-30 MIN	5-10 MIN	1 MIN	0-30 MIN	1-10 MIN	1-5 MIN	9 MINUTES AND UP DEPENDING ON SORTIE RATE
NAVAL PATROLS SURFACE	N/A INFOR- MATION DEPENDS ON EVENT OF CONTACT	30 MIN AND UP INCLUDES INTER- PRETATION	1-5 MIN	1-20 MIN	1-20 MIN	1-3 MIN	1-5 MIN	35 MINUTES AND UP DEPENDING ON NATURE OF CONTACT
SUBMARINE	N/A SPECIAL MISSION TYPE OPERATION	NONE INCLUDED IN TRANSMISSION DELAY	1-6 HOURS	1-20 MIN	1-20 MIN	1-3 MIN	1-5 MIN	1 HR AND UP DE- PENDING ON PATROL ACTIVITY
SHORE BASED SURVEILLANCE	VIRTUALLY CONTINUOUS ONE COMPLETE SAMPLE EACH 1-5 MIN	1-15 MIN	NONE	NONE	NONE	1-10 MIN	1-5 MIN	3-30 MIN

FIG. 4 -(U) TIME REQUIRED TO COLLECT, PROCESS, AND DISSEMINATE INFORMATION

SECRET

than accept the 1/2 to 2 hours delay in transmission of information, the Soviets will employ manned reconnaissance satellites and reduce the delay in unloading the information to a few minutes.

A satellite reconnaissance system is so generalized and collects so many different kinds of information useful to so many different activities scattered throughout the Soviet world, that information will be accepted directly from the vehicle at only a few sites on the ground. Here, the information must be interpreted and individual items addressed to the appropriate consumers. Information useful to the amphibious defense can be recognized automatically, however, and is of very high priority. Delays at this point need not exceed about a minute. The problem of communicating the data to the army processing center in a remote part of the world may be very severe. It can be assumed that the Soviets will have an effective rapid data communications system extending throughout the Soviet Bloc and into any Soviet theater or military operations by 1975. Communications with revolutionary forces or more primitive nations may be limited to radio teletype.

The data processing and transfer problems in aerial reconnaissance are quite similar to those involved with satellite reconnaissance except that the total volume of useful data may be much greater and the surface collection points more numerous. Some of these may be within the army zone and in direct support of the amphibious defense.

Collection, processing and dissemination of information resulting from naval surface patrols is complicated by the fact of their being effective in collecting information to the extent that they engage the amphibious force. Information gained in this way is likely to be fragmentary but also detailed and accurate. It is interesting also because the engagement in which the information is obtained may change the situation.

The shore based surveillance systems provide almost continuous coverage in time and space out to the limits of their range. The preliminary processing involved here is principally correlation of data in time and between sites for the purpose of identifying targets and locating them. This processing may be distributed among the collection sites or at an Army surveillance center or both. In any event the communications links are short and employ facilities devoted to this purpose.

SECRET

Times required to collect, process and disseminate information and to start execution of tactical decision at army level are summarized in Figure 4. Here it is assumed that an effective system for control of collection and dissemination is in operation. Decision times are measured from presentation of the last item of information from among those which cumulatively contributed to it.

Once debarkation or the assault phase starts, commanders at the echelons below army along with the army commander have an immediate requirement for combat intelligence information. Specifically, they need information about

- a. The strength and composition of the assault force.
- b. The points and times at which the landings will be made and have been made.
- c. The enemy's capability to reinforce his troops ashore.
- d. The time and place at which he can land tanks.
- e. Target acquisition information for missiles and artillery.
- f. Fire control information for missiles and artillery.

In addition, the preassault requirements of the army commander continue because he cannot be certain that the assault in progress is his only threat.

All of the shore based surveillance means are effective during debarkation and assault and it can be expected that the collected information will be correlated well and be disseminated efficiently over secure communications links according to a well practiced plan.

Electronic and communications intelligence become more important than in earlier phases because elements of the amphibious force are being forced to react. Ships are under attack and must use radars and guidance transmitters to defend themselves. Extensive command and coordination communications are required within the landing force. Troops ashore must request fire support and reinforcement when and where they need it. All this is conducted by relatively insecure tactical radio.

Once a beachhead is established and a breakout is achieved, the defense becomes a mobile one in which the advance is not frontally opposed but is directed and channelled by means of blocking positions and flank attacks with an objective

SECRET

of pinching off the advancing column, cutting it up and defeating it piece-meal. The whole character of the defense changes from a static preplanned one involving almost no radio communications to a very complex operation in which units leapfrog rearward, armored units are committed to objectives as they appear and radio becomes the principal means for command and control.

SECRET

III. COMMUNICATIONS TECHNOLOGY, 1975-1980

The communications environment to be encountered in the amphibious operation area in the 1975-1980 time period can be estimated by using several factors, as follows: The present environment is a base about which we have good knowledge. From the state of the art of today we can predict certain trends in the environments of the future. In order to arrive at a time factor to bracket the environment of a future time period, some knowledge of the rate of transition of state-of-the-art capabilities to militarily operational systems is necessary. Our standard of measurement here must be varied in accordance with the effort, i. e., money expended to effect this transition. In the absence of some stimulus, the rate of expenditure in a given technological area can be related to the economic growth of a country. Sudden awareness that a potential enemy has developed a capability in which the U.S. was apparently lagging was a stimulus which provided an increase in expenditures in rocket development and the exploration of space. A change in political objectives in one or more of the major countries of the world might, if it affects the status of the "Cold War," change the rate of research and development spending in these and other countries.

The environment predictions which follow are based upon the factors described above. If a study of this sort is to be realistic, the most technically advanced potential enemy country must be used in arriving at this environment. For this reason, the Soviet Union is considered in the making of the following estimates. It is probable that any amphibious operation that the U.S. would make in this time period would not be against the Soviet homeland, but it probably would be against an area under Soviet Bloc control. The extent to which these environmental elements would be found depends to a large degree upon how important they consider the area to be in light of their objectives.

A. USE OF THE FREQUENCY SPECTRUM1. Acoustic Communications

The most common form of acoustic communications is the transmission of intelligence through the atmosphere. This may take the form of voice, whistles,

drums, horns, etc. The use of airborne sounds in deception is common, but little use will be made of it in communications deception.

Acoustic transmission through water is also practical. Enemy defense forces of the future can be expected to use underwater sound detection both with subsurface craft and from shore operated listening stations. This use of Sonar is most helpful in detecting and classifying surface and subsurface amphibious craft. Underwater sound is also used for communications and we should expect the defending forces to be using underwater sensors to monitor for communications as well as for ship noises. Various methods are used to transmit communications through water. CW, teletype, or voice modulation of fixed frequency in either amplitude or frequency can be used. Forms of noise modulation are also useful in providing some degree of security to such communications.

2. Radio Communications

For many years following World War II, military use of the electromagnetic spectrum was confined to continued but expanding use of the frequency range from 2 to 500 megacycles for communications and from 1000 to 10,700 megacycles for radar and microwave services.

The U.S. Navy Polaris program and the expanding need for ASW have caused increased use of the very low frequencies. Communications as low as 14 kc are common. Navigation aids are operating experimentally at even lower frequencies. The Soviet Union is known to be doing extensive work in VLF for both communications¹ and navigation². It is to be expected that work in this area will continue in the Soviet Union and may find extensive use in the 1975-1980 time period for long range communications and navigation work. Communications at the very low frequencies have severe limitation on bandwidth and common practice is to transmit information by morse code or radio teletype. Other approaches must be considered, however, as demonstrated by a U.S. acoustic

¹ CIA, Soviet Very Low Frequency (VLF) Radio Communications, CIA/SI 42-59, 14 October 1959, Secret.

² ONI, Star No. ONI-ST-8-59, 27 January 1960, Secret/Noform.

system for use in conjunction with LORAD Sonar.¹ This system, SESCO, falls in the noise-like pseudo-random category. Transmitted bandwidth is 1 kc but the information bandwidth is only 1 cps.

Although SESCO is an acoustic system, designed for propagation through water, the fact that noise-like pseudo-random techniques are applicable even with highly limited bandwidths is of obvious significance to VLF communications.

The upper end of the frequency spectrum has also seen expanded usage. New microwave developments have spurred the use of frequencies above 10 Gc. U.S. systems as high as 60 Gc (60,000 Mc) are now in operation. Intelligence sources indicate that the USSR is also working in this range today. Radar, communications, and wide band data links are rapidly expanding the use of this portion of the spectrum. With the development of masers and lasers, the tools are now available to expand the spectrum usage even further.

Present Soviet research and development activities indicate that millimeter-wave communications will see tactical use in the 1975-1980 period as follows:

- a. Point-to-point, single-channel, tripod mounted systems for applications such as fire control communications.
- b. Point-to-point, high capacity van mounted systems for trucking.
- c. Ground-air and air-ground communications (in K, Q, V bands) in control of ground support aircraft, support of airborne operations, etc.
- d. The possibility of wide-band relay systems for computer to computer communications also exists, however, this item is not likely to be found in most amphibious operations areas in the 1975-1980 time period.

Continued use will be made of the HF, VHF, SHF bands. Some of the tactical communications uses applicable to 1975-1980 are:

¹ University of Michigan, Cooley Electronics Laboratory, An Introduction to Pseudo-Random Systems, Vol. II, Technical Report No. 10411, September 1963, Secret/Not Releasable.

- a. Single channel, low power HF, VHF and possibly UHF communications. (Millimeter-wave communications as discussed above and optical communications to be covered in the next section supplement this usage.)
- b. Multiplexed, medium and high-power HF and VHF communication are probable.
- c. Tactical (mobile) troposcatter in the VHF region should be available during this period.
- d. Directional radio relay in the VHF, UHF and SHF will be in use. (The possibility of millimeter wave use for this application was mentioned previously. Optical relay is covered in the next section.)

3. Optical Communications

Perhaps the most desirable characteristic of an optical communications system is privacy. A well-designed system provides a strict line-of-sight transmission with no bends, little radiation in undesired directions and a minimal amount of overshoot. It has a low vulnerability to interference from other optical signals and unfriendly ELINT. For example, if a 1° single-channel beam from a 100-watt source located 10 km from friendly territory was transmitted laterally to a station 10 km away, detection more than 1 km away from the receiving station would be difficult.¹ To jam or to gain intelligence from an optical system by unfriendly forces presents an imposing problem and one that may not soon be solved. Other desirable characteristics of an optical system include wide bandwidth capabilities (see Figure 5), narrow beamwidths with little divergence, low to moderate power requirements, little scatter of energy, small size, light weight, and portability.

There are also various undesirable characteristics inherent in an optical communications system; one of these is limited range. Optical signals are subject to absorption by the atmosphere and to scattering by particles in the atmosphere. There are, however, various portions in the optical spectrum where

¹USASA Board Combat Development Study Number CD-11-0J. U.S. - Soviet Comparison: Optical Communications. (U) 31 May 1963 Secret

FIG. 5 - (U) COMPARISON OF RF AND OPTICAL COMMUNICATIONS CHANNELS

BAND	FREQUENCIES	TYPICAL OPERATING FREQUENCY	CHANNEL WIDTH	% WIDTH
STANDARD BROADCAST	.54 Mc TO 1.8 Mc	1 Mc	10 kc	1
VHF TELEVISION	54 Mc TO 88 Mc 174 Mc TO 216 Mc	60 Mc	6 Mc	10
MILITARY UHF	225 Mc TO 420 Mc AND SOME HIGHER BANDS	300 Mc	100 kc	0.03
OPTICAL	3×10^{11} TO 3×10^{16}	3×10^{14}	30 kmc	0.01

absorption is less intense and it is within these areas that the systems will probably operate (see Figure 6). A system operating in these areas and under average weather conditions will not be greatly affected by either atmospheric absorption or scattering, but under adverse weather conditions such as rain or fog, the range will be severely limited.

Another limitation is the strict line-of-sight requirement imposed by optical systems. Nothing can be allowed to obstruct the light beam. This differs from UHF line-of-sight because while foliage and other obstructions hinder operations, they by no means sever it.

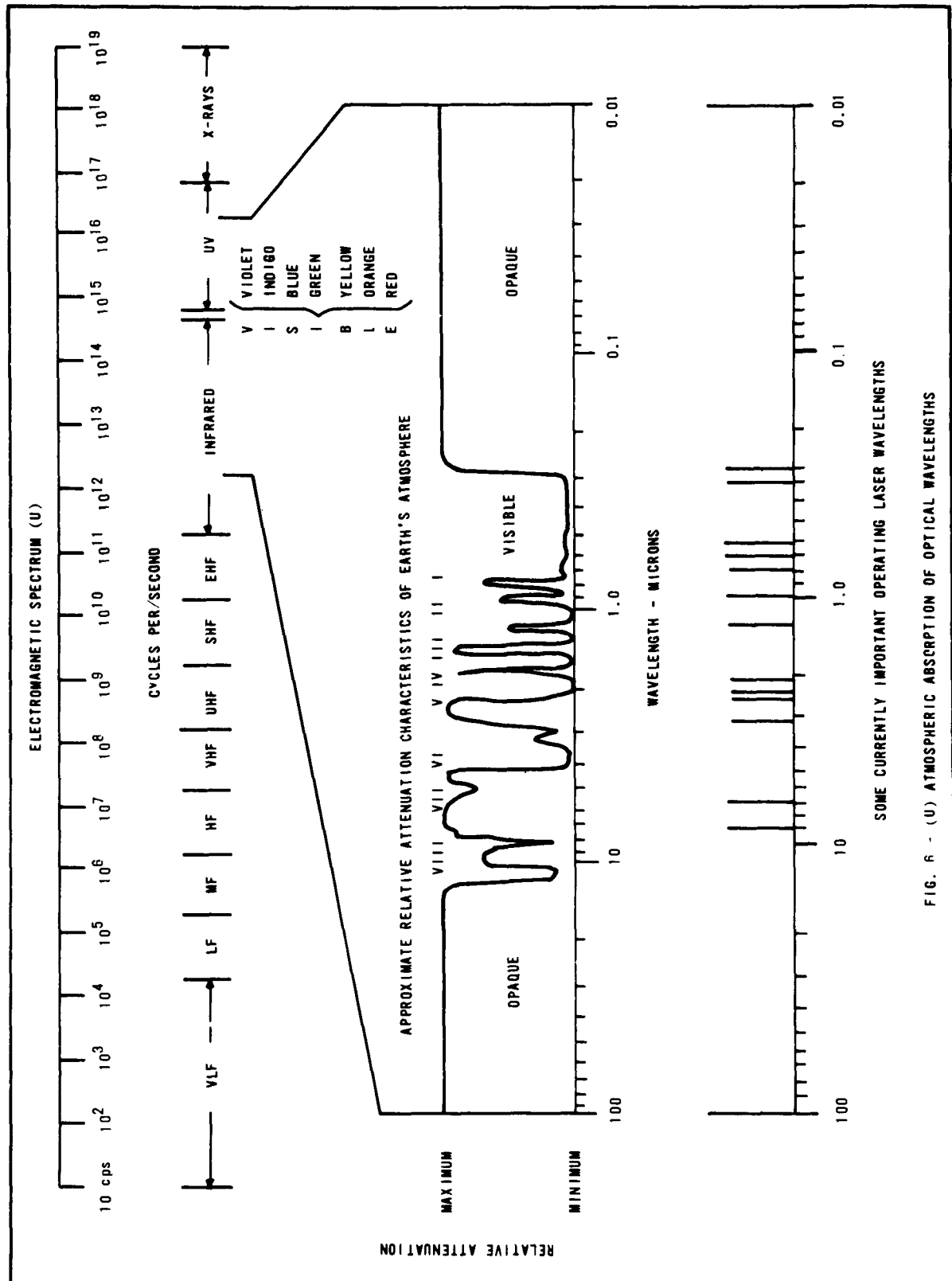
Very narrow beamwidths which are available with optical systems do not create any problems in a fixed point-to-point system, but do cause problems in portable or shipboard systems. It has been shown in tests of handheld optical systems that contact is difficult to establish and even harder to maintain with any reliability, when using a beamwidth of 2° by 3° .¹ Other disadvantages are low overall reliability compared to conventional radio, generally higher cost than conventional radio for at least the next couple of years, additional logistics and maintenance requirements, and insufficient ruggedness to meet stringent JAN specifications.

a. Current Capabilities

Prior to 1960, the only sources available for optical communications systems were non-coherent sources. Systems using these sources and operating in the IR region have been employed by both the U.S. and the Soviets since early in World War II. The present U.S. systems range from the shipboard AN/SAQ-1 which is a manually operated shutter system to the shipboard AN/SAC-5(XN-1).² This system automatically searches for and tracks a signal as long as communications are continued; however, long pauses during transmission destroy the tracking feature. Voice, code, or teletype may be transmitted and the presentation may be either aural or printed. Ranges of about

¹ Northwestern University, "Type 'W' Portable Hand-Held Infrared Optical Telephone," IRTA No. 2674, Marck 1949, (U).

² "Military Handbook, Infrared Equipment, Volume I," MIL-HDBK-250-1, 20 June 1961, Confidential.



10 n miles were obtained for voice during tests. Code transmission ranges were limited mostly by the horizon. The U.S. also has various ground-based IR systems with ranges up to 6 miles under average weather conditions.¹

The Soviets have two shipboard systems: OGON, a manually operated shutter system and LILIE, an experimental E. German system which provides voice communications over a distance of 14 km.² The ASTRA II, a system used by the Soviet Navy during World War II for navigation assistance was followed by modifications called the SOVA and DIVER.² These were primarily for detection, but have communications capabilities. The only indication of a ground-based system comes from a Rumanian Military Journal. The equipment is called "radio-telephone" and is reported to have a range of 20 km.³

There are no reported operable communications systems in the ultraviolet or visible portions of the spectrum by either the U.S. or Soviets, except for manually operated shutter systems. The most recent non-coherent sources are krypton and xenon lamps, and a new experimental multi-electrode, gas-discharge generator called "Enertron." The krypton and xenon lamps have a peak output in the 0.7-1.0 micron spectral region,² while "Enertron"⁴ has a reported variable output from .15-35 micron.

Conventional sources in general will probably prove satisfactory for short range communications systems; however, they are not suitable for long range or high-data-rate-systems. Both the U.S. and the Soviets possess the technological capability to produce optical communications systems, but in the past the U.S. has concentrated on the field of IR sighting and IR mapping while the Soviets have concentrated on night viewing and night driving devices.

¹ "Military Handbook, Infrared Equipment, Volume 2," MIL-HDBK-250-2. Secret

² USASA Board. Combat Development Study Number CO-11-OJ. US-Soviet Comparison: Optical Communications. (U) 31 May 1963 Secret

³ USAF, Air Intelligence Report, 12 May 1961 (U).

⁴ Missiles and Rockets, Vol. 13, No. 17, 21 October 1963, pp. 26-27. (U)

b. State of the Art

The advent of the laser in 1960 promises both long range and high data rate capabilities and since 1960 many advances have been made. The laser, however, is a relatively new device and millions of dollars are being spent by both the U.S. and the USSR on basic and applied research relevant to optical devices (about 200 million by the U.S. during 1962). While only a small percentage of this money was spent to develop communications systems, the overall research cannot help but benefit it.

The laser as it stands today is by no means ready to be put into the field; but with the fast developing technology, both in the U.S. and the USSR, it is expected an optical system using a laser for a source will be operable by the time period in question, 1975-1980.

Optical communications systems are not expected to replace radio and wire communications, but rather to supplement them. There are various situations where optical systems would have high value during both offense and defense operations.

Optical communications systems could possibly be very useful during amphibious landings for secure ship-to-shore traffic. Its disadvantages are that the operating personnel will be more exposed due to the strict line-of-sight requirement and because of the instability of the ship platform, lock and track capabilities will have to be developed.

An optical system may be valuable to both a reconnaissance patrol and a forward observer. Both would be able to remain in a forward position for extended periods and transmit continuously without revealing their presence.

There appears to be little use for optical systems during actual contact with enemy forces because of the fluid conditions that exist at that time; however, they may be useful for the control of troops that are approaching the forward line. In an assembly and reserve area, optical systems could provide unlimited secure communications.

Optical nets could prove to be very valuable for communications between command posts because of the high-capacity and privacy features. Due to relative freedom from intercept, messages may be transmitted without encryption and thereby save time. There is also the advantage of freedom from interference.

A ground-to-air optical net would assure almost complete privacy and an air-to-ground net would be almost as good. These nets could be used for amphibious landings, fire control, and direction of build-up or supply drops. These optical systems would need wider beamwidths and also lock and track capabilities.

The high capacity potential of optical communications systems makes them desirable for use in data transmission and processing nets. These systems could also be used in air defense nets or to communicate between computers.

In general, optical systems could perform many of the functions that radio and wire communications now provide. There are some functions that cannot be performed easily by optical systems (e. g. , long-distance communication), and these systems are limited by weather and a strict line-of-sight requirement. For a good portion of the time, however, optical nets could significantly reduce the amount of radio communications traffic thereby reducing interference with other communications.

B. MODULATION TECHNIQUES AND OPERATIONAL CAPABILITIES

Modulation is the addition of information to a carrier wave. This carrier wave may be acoustic, electromagnetic, or optical in character.

In general the information modifies the carrier in one of two ways. In one the amplitude of the carrier wave is varied in accordance with the information added. In the other the frequency of the carrier wave is varied. These are referred to as amplitude modulation (AM) and frequency modulation (FM). A third form, phase modulation, varies the instantaneous phase of the carrier wave but the signal produced closely resembles FM. For this reason it will be grouped with FM in this discussion. Likewise CW (such as Morse code) with on-off keying is considered amplitude modulation. In this case only two discrete amplitude levels are produced; i. e. , carrier full on or off.

Other forms of modulation exist which are outside the two general types above (for example pulse modulation) and others are difficult to classify under a single heading. Some of these will be discussed where they may be applicable to the communications deception effort in the amphibious operation area for

the 1975-1980 time period. Figure 7 shows the classical definition for various modulation types along with the symbolic notations which are common at the present time in the United States.

Modulation types to be anticipated in the amphibious operations area during the 1975 to 1980 period will be similar to and outgrowths from the forms now used. The sophistication of modulation types will depend to some degree upon the security required in the transmission. For front line tactical use, we can expect the defending forces to use plain text voice communications with some simple form of verbal codes for such things as map sectors and well established plans. These communications will likely be carried over telephone/wire circuits and there is little likelihood of causing deception in these channels before or in the earliest phases of the assault operations. Low power voice radiotransmissions will be confined to scouting parties, and hastily established reconnaissance positions. These will probably be VHF circuits. As an amphibious operation gets underway, some of the telephone circuits will be disrupted by bombardment, or by movement of the enemy troops. At this time the use of VHF circuits will increase. Forces on the move must have communications and wire service is impractical. Similarly, each level of command and control has problems which dictate to a large degree, the type of communication to be expected at various times throughout amphibious operation. In a tactical operation, where time is a critical element, plain text voice communications can be expected. Likewise, the frequency range to be used will be determined to a large extent by the distance it is expected to encounter.

Soviet military communications in the VHF bands in 1963 use a mixture of FM and AM modulation. Older equipments are AM and newer units are FM. By 1975 most of the AM equipments will probably be replaced by FM units, with the possible exception of aircraft communications. HF band communications are also used by the Soviets at the present time. A trend is noted here in the change from amplitude modulated voice to single sideband voice (A3a).

Higher echelon units have different communication requirements than the front line units. They must communicate with stations which are farther away and also their messages may not be of immediate urgency. There is also at times a requirement for hard copy. Encrypted communications are most commonly sent by CW or teletype. A1 emission is commonly used for long distance CW

TYPE OF MODULATION	TYPE OF TRANSMISSION	SUPPLEMENTARY CHARACTERISTICS	SYMBOL
AMPLITUDE MODULATION	ABSENCE OF ANY MODULATION		A0
	TELEGRAPHY WITHOUT THE USE OF MODULATING AUDIO FREQUENCY (ON-OFF KEYING)		A1
	TELEGRAPHY BY THE KEYING OF A MODULATING AUDIO FREQUENCY OR AUDIO FREQUENCIES, OR BY THE KEYING OF THE MODULATED EMISSION (SPECIAL CASE: AN UNKEYED MODULATED EMISSION)		A2
	TELEPHONY	DOUBLED SIDEBAND, FULL CARRIER	A3
		SINGLE SIDEBAND, REDUCED CARRIER	A3a
		TWO INDEPENDENT SIDEBANDS, REDUCED CARRIER	A3b
	FACSIMILE		A4
	TELEVISION		A5
	COMPOSITE TRANSMISSIONS AND CASES NOT COVERED BY THE ABOVE		A-9
	COMPOSITE TRANSMISSIONS	REDUCED CARRIER	A-9c
FREQUENCY (OR PHASE) MODULATION	ABSENCE OF ANY MODULATION		F0
	TELEGRAPHY WITHOUT THE USE OF MODULATING AUDIO FREQUENCY (FREQUENCY SHIFT KEYING)		F1
	TELEGRAPHY BY THE KEYING OF A MODULATING AUDIO FREQUENCY OR AUDIO FREQUENCIES, OR BY THE KEYING OF THE MODULATED EMISSION (SPECIAL CASE: AN UNKEYED EMISSION MODULATED BY AUDIO FREQUENCY.)		F2
	TELEPHONY		F-3
	FACSIMILE		F4
	TELEVISION		F5
	COMPOSITE TRANSMISSION AND CASES NOT COVERED BY THE ABOVE		F9
PULSE MODULATION	ABSENCE OF ANY MODULATION INTENDED TO CARRY INFORMATION		P0
	TELEGRAPHY WITHOUT THE USE OF MODULATING AUDIO FREQUENCY		P1
	TELEGRAPHY BY THE KEYING OF A MODULATING AUDIO FREQUENCY OR AUDIO FREQUENCIES, OR BY KEYING OF THE MODULATED PULSE (SPECIAL CASE: AN UNKEYED MODULATED PULSE.	AUDIO FREQUENCY OR AUDIO FREQUENCIES MODULATING THE PULSE IN AMPLITUDE.	P2d
		AUDIO FREQUENCY OR AUDIO FREQUENCIES MODULATING THE WIDTH OF THE PULSE.	P2a
		AUDIO FREQUENCY OR AUDIO FREQUENCIES MODULATING THE PHASE (OR POSITION) OF THE PULSE	P2f
	TELEPHONY	AMPLITUDE MODULATED	P3d
		WIDTH MODULATED	P3a
		PHASE (OR POSITION) MODULATED	P3f
	COMPOSITE TRANSMISSION AND CASES NOT COVERED BY THE ABOVE		P9

FIG. 7 - (U) CLASSICAL DEFINITION OF MODULATION TYPES

circuits. A2 is required if the recipient is using equipment intended for voice reception primarily. Radio teletype uses frequency shift keying in the HF bands (F-1) and audio frequency shift keying (F-2) in the VHF and higher bands.

Radio teletype provides immediate printed hard copy and with the use of on-line encoders and decoders little time is lost in providing security.

Security can be provided in voice communications by speech scrambling, pseudo-noise transmission and other techniques. Speech scrambling is a method of breaking up the components of speech and reassembling them in a frequency displaced order prior to transmission, then reassembling them into original order at the receiver. The transmission can be AM, FM, SSB or any of the voice modulation modes. Scrambling has been used since the 1930's and probably will continue to be found through 1980.

Pseudo-noise transmission provides security in that the signal is very hard to detect on a communications receiver. It is a broad band signal that sounds to the operator very much like noise and is frequently missed. Without especially designed receiving equipment it is impossible to extract the intelligence from the signal if it is detected.

Burst transmissions are another form of communications which are intended to provide a form of security. The message to be transmitted is first recorded at a normal speed (RTTY or CW), then the entire recorded message is transmitted at a very high rate of speed. At the receiving station the off-the-air signal is recorded at high speed, then played back at the normal speed to extract the intelligence. This reduces transmission time to seconds and the probability of interception is greatly reduced. Even if it is intercepted, the signal is on for such a short time that locating the transmitter by radio direction finding is extremely difficult. There is little likelihood of this type of signal being used by land forces during an amphibious operation, but a reconnaissance submarine operating in the area might use it to report on U.S. activities.

A form of modulation peculiar to optical or laser communication is polarization modulation. To achieve modulation of this sort, the light output from the source is passed through a polarizing filter which is capable of having the polarization changed in accordance with the intelligence which is to modulate the signal. In laboratory practice today this is done with a Kerr cell. At the

SECRET

receiving end of the communications link, fixed polarizing filter has been placed in front of the detector and adjusted to provide little or no output when no modulation is present at the light source. As the polarization of the source light is modulated with intelligence, the rotation of the polarized light beam will cause variations in the amount of light passing through the fixed filter at the receiver. In this way the detector in the receiver can recover the intelligence from the light beam.

SECRET

IV. COMMUNICATIONS DECEPTION

Communications deception is a vital part of an amphibious assault deception plan. It must be closely associated with the overall deception plan of the group.

Tactical communications deception can be conveniently divided into two categories, Manipulative and Imitative. Manipulative deception is the use of friendly communications in such a manner as to falsify the information which a foreign nation can obtain from their analysis. Imitative deception is the intrusion on the enemy's communications circuits and the imitation of his traffic to produce a desired result.

Several other factors are closely related to communications deception. Denial of information to the enemy by the use of radio silence, secure communications systems and cover are deception aids. Jamming of the enemy's communications disrupts his functions and may cause delays in the reception of information vital to the defense of the area being assaulted.

Navy amphibious warfare operations can be separated into several phases:

1. Planning
2. Embarkation
3. Rehearsal
4. Movement to Objective
5. Assault
6. Consolidation at Objective

Communications deception as considered in this study of the 1975-1980 time period is primarily concerned with activities in the Assault phase. It is recognized that some strategic communications deception has probably been practiced prior to this phase in order to avoid alerting the enemy. Special security precautions are also used in the various phases prior to the assault phase. Radio silence is maintained while at sea. Upon arrival in the objective

area radio silence is lifted for the express purpose of establishing essential radio nets. This is the earliest possible time for the use of tactical communications deception.

A. MANIPULATIVE COMMUNICATIONS DECEPTION

Manipulative communications deception may be strategic or tactical. Strategic deception in Navy communications is predominantly practiced and controlled at a higher level of command than that associated with tactical deception. One of its main uses is to conceal the buildup and departure of fleet units.

A common method is to include dummy traffic on all circuits likely to be intercepted and analyzed by enemy intelligence. When a proposed operation requires that additional communications be handled on these circuits, the required messages are substituted for dummy messages resulting in a uniform volume of traffic. When the amount of traffic which must be handled in connection with a large operation exceeds the volume of dummy traffic normally carried on a given circuit, lower priority traffic is shunted from this circuit for delivery by other means. These efforts prohibit enemy intelligence from being alerted to a possible impending operation due to analysis of traffic volume.

Tactical communications deception is authorized for use under the direction of fleet or task force commanders when in actual contact with an enemy if the deception will affect only the tactical situation.

Manipulative communications deception in the objective area is used in connection with other deception action including radar deception, sonic deception, visual deception, navigation deception and others. These deception tactics in an amphibious assault operation are carried out aboard one or more ships or small boats which are sent away from the main task force to simulate an attack at a point other than the real objective. This may be as a feint or as a diversion. Communications deception equipment on these platforms simulate the communications of the task force in an attempt to divert some of the enemy strength. The use of deceptive radio transmissions along with electronic and other deception equipments simulate large forces preparing to make an amphibious assault. The communications of the main task force must be secure during this deception effort in order to be reasonably certain that the enemy will be deceived.

Timing of the deception effort must allow the enemy to detect, evaluate, and initiate the intended action. For the deception to be effective the enemy must be capable of reacting as intended in the time available.

Conventional transmitters and receivers can be used for communications deception; however, types and characteristics must match those of the ships which are being simulated. Multichannel tape recorders are normally used to control the deception transmitters. In voice circuits the transmitters are keyed by voice controlled relays directly from the tape recorder. Tapes are prerecorded, often during other amphibious operations, with appropriate modification having been made to provide proper reference to time, date, and location. When possible the recordings are made of transmissions from the actual ships they are intended to simulate. In this way voices of actual operators passing actual communications are created with preservation of time within a net and between the simulated nets controlled by other channels of the same tape. At the present time seven channel tape recorder/reproducers are employed providing seven deception nets from one tape. Each channel controls a single transmitter which simulates an entire net. One twelve inch reel of 1/2 inch tape can supply 12 hours of continuous operation. If the tapes are recorded from receivers monitoring the appropriate nets the audio quality and audio characteristics of the individual net transmitters are reproduced during the deception efforts.

In the 1975-1980 time period it is probable that enemy intercept operators will have automatic, real time, analysis equipment to examine characteristics of the transmitted signals. Several characteristics which might be examined to identify deception transmissions of today are:

1. Build-up of the carrier wave in the first few milliseconds after the transmitter is turned on.
2. Length of time after carrier activation before the operator begins to speak.
3. Length of time after operator completes his message before he turns off the carrier.
4. Decay time of the carrier wave on turn-off.

5. Precise measure of frequency difference between different transmissions. Items 1, 4, and 5 are characteristics of the transmitter. They will vary from transmitter to transmitter but will remain substantially constant for a given transmitter.

Items 2 and 3 are characteristics of the operator. They will vary greatly from operator to operator. They will not remain constant with a given operator, but similar trends can be observed as operator identifiers.

Another system which may be available to the intelligence monitor of a more sophisticated enemy in the 1975-1980 time period could provide near instantaneous position locations of radio transmitters over a wide frequency spectrum. If the resolution of such a system is fine enough, he may be able to determine that all transmissions are coming from an area too small to contain all of the apparent ships represented on the network.

The use of light, IR, and other non-radio communications in the assault operation will probably increase in the future. Forms of communication more secure than radio will be used whenever possible for actual assault operations. These primarily give the desired amount of communications with less chance for enemy interception. If it is believed that the enemy has become aware of these communication methods, some attempt should be made to include deception systems of these types in the advent that the enemy has developed some means of observing them.

B. IMITATIVE COMMUNICATION DECEPTION

Imitative communication deception involves intentional intrusion into an enemy communication system for the purpose of introducing false or misleading information. The information introduced has the purpose of placing the enemy in a position or state of mind favorable to the attacking force. How effective imitative deception will be depends on factors such as combat situation (intense, stable, etc.); message authenticity; the appropriateness and reasonableness of the message; the skill of U.S. operators in portraying the enemy operators; and how cautious, occupied, fatigued, or harrassed the enemy operators are.

Imitative communication deception will have little or no use in any phase of an amphibious operation except for the assault phase and subsequent operations on land. In any earlier phase of the operation, imitative deception would have minimum possibilities of success. The defending forces would be in a static condition but expecting an assault somewhere along their perimeter. At this time, very little confusion would exist among the enemy operators and they would tend to be cautious and suspicious. There would be time to require authentication for any and all messages and time to check the message if authentication is not received. The enemy operators would generally know each other and would question the presence of an unknown operator on the net.

There is also the interaction of imitative deception and communications intelligence to be considered. Communications intelligence supplies the information about the characteristics of the enemy's communication equipment. Successful imitative deception or an unsuccessful attempt at imitative deception prior to invasion, if realized by the enemy, would infer the success of our communications intelligence effort and tend to cause the tightening of the enemy's communication security. Also, the effort required to mount an effective imitative deception operation might indicate that an important activity was taking place, or about to take place.

The Soviet communications doctrine emphasizes security, therefore, the most probable communication systems will be wire, microwave, and fixed point-to-point systems using millimeter or optical devices with radio as a backup. Generally, imitative deception will not be effective against communication systems other than radio because of the difficulty of intruding in those systems. Therefore, for planned targets of imitative deception, the effort should be concentrated against radio nets. Nets using other systems would be targets of opportunity.

If imitative communication deception is to be used against higher echelon nets, the cost of such an effort should be evaluated carefully against the very possible loss of information sources if the deception is realized or if the effort is unsuccessful. Against lower echelon nets, however, little is lost if the deception effort is realized. Higher echelon nets will also be less susceptible to imitative deception due to the type of system used (wire, optical

devices, etc.); type of communication technique (burst, pseudo noise, etc.); authentication procedures, and the security of the messages (crypto). The immediate problem of the imitative deception effort against a defense then is to get the lower echelon nets to use radio communication. The weather (natural or induced) at the time of the invasion may be such as to require the use of radio communications or the "softening up" of the landing area may destroy or disable some of the nonradio systems, thus requiring the use of radio. If measures such as these do not force the enemy to shift to radio, the eventual overtaking of some front line positions by the invading force with the corresponding withdrawal of the defenders will cause some use of radio.

1. Intrusion Techniques

There are various techniques that can be used to intrude on an enemy's radio net.

a. Techniques Against Nets with Poor or Nonexistent Authentication Procedures

(1) The simplest and most direct technique would be to enter a net and assume the position of an out-station or control station. The intruder would not attempt to authenticate his messages for in fact he would probably not know the authentication procedure. The success of the intrusion would depend upon the neglect of the enemy operators to demand proper authentication.

The effectiveness of this technique against U.S. forces was illustrated by the U.S. Fall Battle Group Efficiency tests in Korea during 1958. The results of these tests were:¹

"1. Number of ICD attempts - 127.

2. Number of times messages were accepted by Battle Group Stations - 119.

¹Letter of Chief Signal Officer, Dept. of Army, Washington 25, D.C. from Hq. USARPAC, Subject: "Communications Vulnerability," January 1959 (C), enclosure to Chief U.S. ASAPAC from 321st U.S. ASA Bn, APO 358 through Commanding Officer, 508th U.S. ASA Group, Subject "COMCM Testing After Action Report," Confidential.

3. Number of demands for authentication - 43.
4. Number of times messages were refused by Battle Group Stations - 14.
5. Number of messages receipted for by ICD without authentication - 28.

"The general reaction of ICD message injection ranged from fairly good to dangerously poor. Of six Battle Groups tested, operators from only one Battle Group consistently and properly utilized authentication tables. One other Battle Group reacted in better than average manner. The remaining four Battle Groups were extremely vulnerable to anyone caring to enter their nets.

"In one instance the ICD team twice took over the Battle Group Command Net as Net Control Station for a period in excess of three hours. The entire net accepted false orders to change frequencies on one occasion. The entire Battle Group POL distribution plan was advanced by eight hours on another occasion. Every false ICD message was accepted without question or request for authentication until the ICD team, acting as an out-station, refused to accept its own message. Although the false messages were relatively harmless, they indicated the vast amount of damage an English speaking enemy operator might have accomplished. One station's firm demand for proper authentication would have prevented several hours' net control by an alien operator.

"On at least 24 different occasions, ICD operators firmly established themselves in nets, often as Net Control Stations. Only twice throughout the problems were there demands for authentication. Casualty reports, troop movements, supply status, and communications information were freely revealed with no attempt toward verification. In one case, ICD operators had to jam a cavalry operator's frequency to prevent his revealing specific coordinates."

(2) If SSB is being used, modulate the sideband opposite to that employed by the enemy's circuit and send the deceptive message at a higher power level. The deceptive message will either drown the valid message completely or the receiving enemy operator, hearing two signals, may assume the weaker signal is from a distant net operating on the same frequency and accept the stronger deceptive signal.

b. Techniques Against Nets with Good Authentication Procedures

(1) Sudden intrusion and insertion of a message into a net with the message directed to no one in particular. The method of delivery and the message context are depended upon to deceive the enemy as to identity of the source and the validity of the message. This technique would be used mainly to instill emotional states.

(2) Transmission of the message with continual interference so as to make the beginning and end of the message unintelligible but allowing the primary contents of the message to get through.

(3) Simulation of equipment malfunction by fading in and out but again allowing the main context of the message to get through.

(4) Using the principle of FM capture, transmit immediately upon the start of a valid transmission and terminate when the valid transmission ends.

(5) Intrusion on two nets simultaneously. When challenged on one net present that challenge on the other net. When authentication is received, use it on the first net.

2. Aims of Imitative Communication Deception

Once the enemy's radio communications network has been successfully intruded upon, the intruder will introduce certain information which will cause particular results in the enemy's behavior. The results of the messages or suggestions are, of course, dependent upon the aim of the intrusion. Four aims have been isolated: (1) the inducement, reinforcement, or expansion of morale or emotional states; e.g., fear, depression, disillusionment, etc.; (2) the instillment of confusion; (3) the commitment, diversion, or dispersement of enemy forces and/or equipment; and (4) the delaying and/or impairing of the enemy's communications.

It should be noted that the defending force, presumably Soviet or Soviet Bloc, has had little experience in amphibious warfare. It should also be noted that, barring the outbreak of a general war or limited wars before 1975, most of the enemy forces in the time period in question will have had little actual combat experience. Due to this lack of experience and knowledge of the assault force, the enemy will have feelings of fear, anxiety, and apprehension. These feelings

can be exploited by a skilled imitative communications deception effort.

The introduction of confusion into the enemy communications nets will have the effect of delaying military decisions because the enemy commanders will begin to question the accuracy of the information which is furnished to them via these communication nets. Attempts by these commanders to obtain verification of messages will introduce further delays. The lower echelons will question the authenticity of the command messages and may delay their response to legitimate commands while they attempt to obtain verification.

One effective method of introducing confusion, for example, is the insertion of messages which indicate the loss of command. If this type of intrusion deceives the lower echelons, the commanders at these lower levels may suspend effective action to wait for further orders for competent authority, or they may even abandon resistance altogether. Another effective intrusion technique is for the intruder to represent himself as net control and issue an order, and then to re-enter the net with the assertion that the order was transmitted by an intruder and to ignore it. This makes it difficult for the real net control station to resume control.

All of these intrusion techniques which are designed to introduce confusion, of course, depend upon the achievement of a high degree of authenticity by the intruder. This means that the intruder must possess a great deal of prior information concerning the enemy tactical radio procedure, command organization, etc., as well as intimate familiarity with the enemy language and even his cultural milieu.

The prime objective of any imitative deception effort should be the control of enemy troops and/or equipment. But this is always difficult to achieve directly and may be at times altogether impossible. Even on a net where authentication procedures are not being enforced, the intruder cannot simply expect to order an enemy to change its status even though the order might be tactically sound from the enemy's immediate standpoint. Even during the greatest confusion a commander would be reluctant to change his status without further checking on the validity of the order. An indirect approach, however, is feasible.

The higher echelon commanders base their tactical decisions on the intelligence information transmitted from the front lines. To intrude on these intelligence nets themselves would be extremely difficult because of the security of the nets. The information passed on these nets, however, could be the result of a successful imitative deception effort. Once the deceptive message or idea is accepted by the front line commander it then becomes fact and is transmitted as such to the higher echelon commanders. Even though this information may be contrary to other information received from the front lines, it may cause the commander to make a wrong decision or to delay his decision until further information is received. Either one of these results could be very advantageous to the assaulting forces. Therefore an imitative deception effort against the enemy's front line forces using a combination of confusion, psychological conditioning, discrete coordination of imitative communication deception and jamming, and appropriate messages could cause movement or non-movement of enemy front line and/or reserve forces.

Any intrusion in an enemy's net denies him full use of the circuit. The minimum effect of the first three aims of imitative deception would accomplish this, however, there are other techniques which could be used to specifically delay or impair enemy communications. Imitative deception used as a jamming measure could be more effective than an ordinary jamming technique to impair communications, e.g., spot jamming, because imitative deception is perhaps less vulnerable to quick identification by the enemy. The intruder could:

(1) Intrude into a RTTY net and during the transmission of a message send a test signal which uses all of the characters, e.g., RY's. The enemy operator would tend to think that his equipment has drifted off frequency because of the incoherence of the message and would try to adjust his set. The result of this technique would be the nonreceipt of a message and the corresponding retransmission of the message or messages. Used discriminately this technique could be effective for a period of time without being detected.

(2) Retransmit previously recorded messages with appropriate heading and date-time groups.

3. Requirements for Successful Intrusion

It is one thing to intrude on a net and communicate messages and suggestions, but it is another to get the enemy to accept them. In order to enhance the possible success of an imitative deception effort, several points must be taken into consideration.

a. Message Content

Especially for the inducement of morale or emotional states the following should be considered:

- (1) The enemy's particular social (including home life), religious, and political beliefs and ideals.
- (2) The recent social or political events, both on a local and national scale.
- (3) Status of the war effort, both on a local and national scale.
- (4) The enemy's local (assault location) situation and environment, incapacities and capabilities.
- (5) The enemy's peculiar personality traits.
- (6) The possible adverse effects of the induced morale or emotional states.

Other considerations should include

- (7) The appropriateness and reasonableness of the message.
- (8) The time required to obtain desired results.
- (9) Enemy net structure.
- (10) The position and status of the enemy's commanders.

b. Communication Skills

The message is, of course, communicated in the enemy's language. However, to insure simulation, the intruder should use the dialect, slang, colloquialisms, and idioms of the enemy. He should also know the conventional

operating procedures and designations and have some idea of the authentication procedures. He must also use convincing emotions appropriate to the aim and content of the message. Good acting and linguistic ability are important requirements.

Of equal importance is the requirement that the intruder have the knowledge to operate and the access to either U.S. equipment having the same characteristics as the enemy's equipment or actual captured equipment.

c. Interaction and Coordination

Successful imitative deception infers the success of our communications intelligence. Because of this fact each attempt at imitative deception should be evaluated carefully for its possible consequential effect on the communications intelligence effort.

Complete coordination is also needed between imitative deception and communications intelligence for several reasons.

- (1) Effective imitative communication deception depends in part on the information obtained by communications intelligence.
- (2) So that communications intelligence will not try to analyze the imitative communication deception signal.
- (3) To measure the effectiveness of the imitative communication deception effort.

4. Imitative Deception Against Non-radio Communication Systems

Non-radio communication systems should be considered targets of opportunity rather than planned targets because of the disposition of the systems, the difficulty of gaining intelligence from the systems, and the difficulty of intrusion. In order to gain sufficient intelligence information to enable effective imitative deception during the assault phase, agents and equipment would have to be placed behind enemy lines for some time prior to the assault to locate and monitor the nets. In view of this requirement it appears that the cost of enemy detection of these agents would be large in comparison to the possible effectiveness of an imitative deception effort. However there may be times during the assault phase where the opportunity for imitative deception would exist. For

example, a sudden thrust by the assault force may cause the capture of an out-station using wire communication before the enemy operator has a chance to inform the other members of the net. But here again, trained personnel will have to be available to perform effective imitative deception.

C. JAMMING

Jamming is not strictly a deception technique but does come into consideration as a related item. Some of the same equipments used for deception are usable for jamming. Some of the imitative deception objectives are duplicated in jamming.

Communications jamming can take many forms. One of the most effective forms for use in the assault area is the interference of communications by interjecting carriers, noise, test signals or other meaningless signals on the radio frequency of the enemy communications net. This is effective against voice, CW, teletype, facsimiles and other communication signals. Special modulation characteristics can be selected to counter each form of information transmission.

Jamming can be done in such a way that it is not easily recognized by the enemy as deliberate, or it can be very deliberate. Jamming may also be used with imitative deception to make it difficult for the enemy to determine if a station is on the enemy net or is an intruder. Voice recognition and other sources of authentication may be countered by increasing jammer intensity at appropriate times, as during authentication requests, and lowering it during transmission of the messages which one wishes to interject into the net. Normally, however, complete jamming will be used only as a last resort, since, in almost every situation, it is of lesser value than either imitative deception or passive intelligence collection.

Jamming of data transmission systems can be distinguished as three types: spot jamming, broadband or barrage jamming, and deceptive jamming. Spot jamming entails the selective masking of an emitter's signals in a particular bandwidth, which focuses a great amount of power on a receiver and ensures jamming within that frequency range. Broadband, or barrage, jamming implies the coverage of a wide band of frequencies by the jammer either through rapid

sweeping of the band or continuous coverage of the target emitter's total frequency range. Deceptive jamming includes the insertion of false or misleading information into an enemy's receiver (the imitative deception technique) or changing the characteristics or parameters of the information being received. Since ICD has been covered in a preceding section of this report, it will not be covered here. The jamming requirements and operational problems encountered in jamming data transmission, noise, and single and double-sideband communications systems are considered in the following paragraphs.

Data transmissions are characterized by pulse trains containing relatively short duration pulses. This characteristic makes accurate measurement by intercept operators of the radio frequency and bandwidth of the emitted signal difficult. Moreover, because precise measurement of either the modulation or the data rate is required, and because all potential bandwidth may not be utilized by the transmitting station, accurate determination of the signal bandwidth poses an additional difficulty.

Unless an ECM effort is certain that the entire bandwidth of a data transmission is being jammed, the intended recipient of the transmission may receive sufficient intelligible information. Completely effective jamming could be provided by a spot jammer concentrating its entire output over the exact bandwidth of the transmitted signal. However, successful spot jamming requires knowledge of the center frequency and effective bandwidth of the signal to be jammed, both of which may be difficult to obtain without a look-through capability. Therefore, broadband jamming, which does not require precise determination of the emitter's RF and bandwidth, is generally more suitable for electronic warfare against data transmission systems, provided that adequate power output is achieved.

Deceptive jamming against data transmission systems, though difficult to accomplish, could be very effective in a tactical situation. Data transmission systems are likely to be used at high levels for important communications; insertion of false information could therefore create grave confusion on the part of the enemy. Major deterrents to the use of such deceptive jamming are the requirements for knowledge of the system's coding characteristics, radio frequency, subcarrier frequencies, and data rate. In addition, the intruder must have transmitting equipment similar to that of the enemy, knowledge of his schedule of operations and generally, information on location of the receiving station.

The major problem presented to an ECM unit by enemy use of noise communications is the extreme difficulty in determining the presence of a communications signal within a band of noise. One approach to this problem is to look for increases in the "signal level" of a band of noise whose average level has already been measured. Should a coherent noise communications system be detected by this method, signal analysis could be performed on the band of noise directly when received.

If, on the other hand, a noncoherent noise system is being used, problems for the jammer are greatly magnified. In order to determine the presence of noncoherent intelligence in a band of noise, the intercept unit may submit the noise to autocorrelation analysis. Although this type of analysis can be performed mechanically, the need for rapid results implies the use of a computer. In addition to these difficulties, successful autocorrelation analysis, though indicating the presence of intelligence in noise, does not necessarily demodulate it. If a requirement for demodulation exists because jamming is to be selective, the intercept group must combine the intercepted signal with a pattern of random noise identical to that programmed for use by the intended recipient of the transmitted noise. If collateral intelligence is not available the determination of the pattern of random noise requires a time consuming systematic process of elimination.

Another adverse feature involved in autocorrelation analysis is the time lag created by the analysis process, even though a computer is used. For example, if the communication undergoing analysis is short, this lag for analysis precludes jamming it. Moreover, information obtained from the analysis process is useful in the future only if the transmitting station continues to transmit messages in the same manner.

The use of a spot jammer against noise communications systems appears to be infeasible. Spot jamming requires determination of the transmitted signal's bandwidth. But in the case of a noise transmission, additional noise in the vicinity of the transmitted band and intercept system noise preclude this measurement unless autocorrelation is performed. This introduces the time lag discussed in the preceding paragraph.

Broadband jamming is, therefore, potentially more effective. It must cover a sufficiently large portion of the spectrum to ensure jamming of the entire bandwidth of the noise signal. However, because the intelligence-bearing components

of one type of noise signal are many and scattered throughout a large bandwidth, a conventional broadband jammer may be ineffective in this case. To meet this problem, the broadband jammer must generate noise containing at least as many frequency components as the communications transmission. The jammer power at each of these frequencies must be greater than that of the target transmitter at the victim receiver. The power required to do this is probably greater than that tactically practicable, at least during the short-range period.

The insertion of a deceptive message in a noise communications circuit at present appears impossible. A deceptive technique, however, could involve the intrusive transmission of a specific noise modulation pattern to superimpose or add to that of the communications transmission. Demodulation of this "doubled" transmission by the receiving station would result in a garbled message. However, this result would automatically indicate the presence of a jamming effort.

Generally, the single-sideband and double-sideband (SSB and DSB) techniques involve suppression of the carrier frequency and transmission of the remaining sideband or sidebands. In the case of SSB, one of the sidebands is also suppressed. In both instances, message reception must be by means of a receiver that reinserts the carrier after signal detection. For optimum performance, the reinserted carrier should be within 10 cps of the original, but deviation of up to 50 cps is feasible. In addition, the amplitude of the reinserted carrier must maintain the same percentage of modulation as occurred at transmission.

In a communications circuit the values of these variables are predetermined and constitute no problem. An intercept group, on the other hand, must establish signal parameters as a preliminary to jamming. Requirements include receiver equipments designed for detection of SSB and DSB signals. Such signals can be detected with conventional AM receivers with BFO (Beat Frequency Oscillator); however, frequent retuning is required to compensate for oscillator instability. Once a signal is detected, the intercept operator must determine the carrier frequency. Determining the proper proportion of carrier level to received sideband, and other demodulation prerequisites appear to be a time-consuming chore rather than a technical difficulty.

Once the tasks involved in signal intercept are completed, jamming of SSB and DSB signals is relatively uncomplicated. Determination of the carrier frequency provides the exact bandwidth of the transmitted signal. Also, because

the bandwidth of a voice communication is fairly narrow (4 kc or less in the case of SSB; 10 kc or less for DSB), jammer requirements are well satisfied by a spot jammer. A broadband jammer is also applicable.

SSB transmissions are vulnerable to at least one type of deceptive jamming. This can be accomplished by generation of the sideband opposite to that employed in the communications circuit. If this spurious sideband is modulated with deceptive information and beamed at an SSB communications circuit receiver at a higher power level than that of the bona fide signal, at least two results may occur: a) the spurious signal, being at a higher power level, will drown the valid communication completely, or b) the receiver operator, hearing two signals at different levels, will assume that the weaker is from a distant communications net operating at the same frequency and place credence in the deceptive message. In neither situation should it be readily apparent to a communications receiver operator that jamming is taking place.

V. ENEMY ANTI-DECEPTION ACTIVITIES

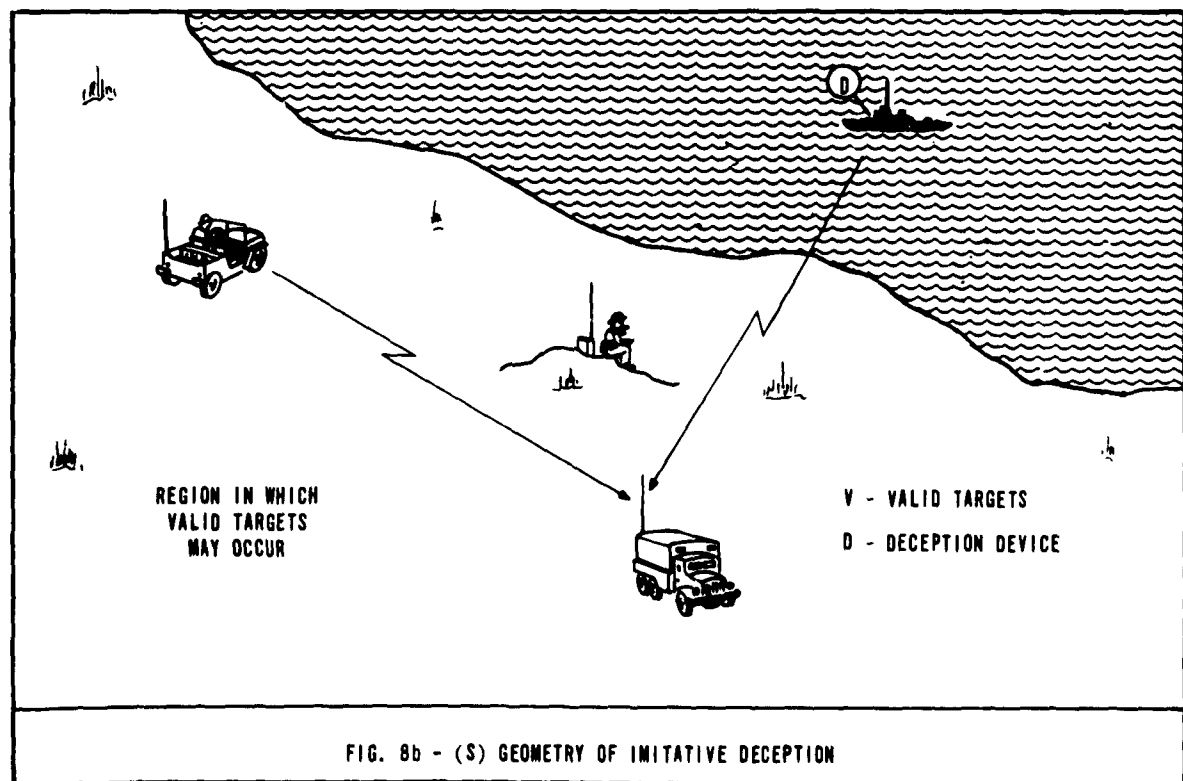
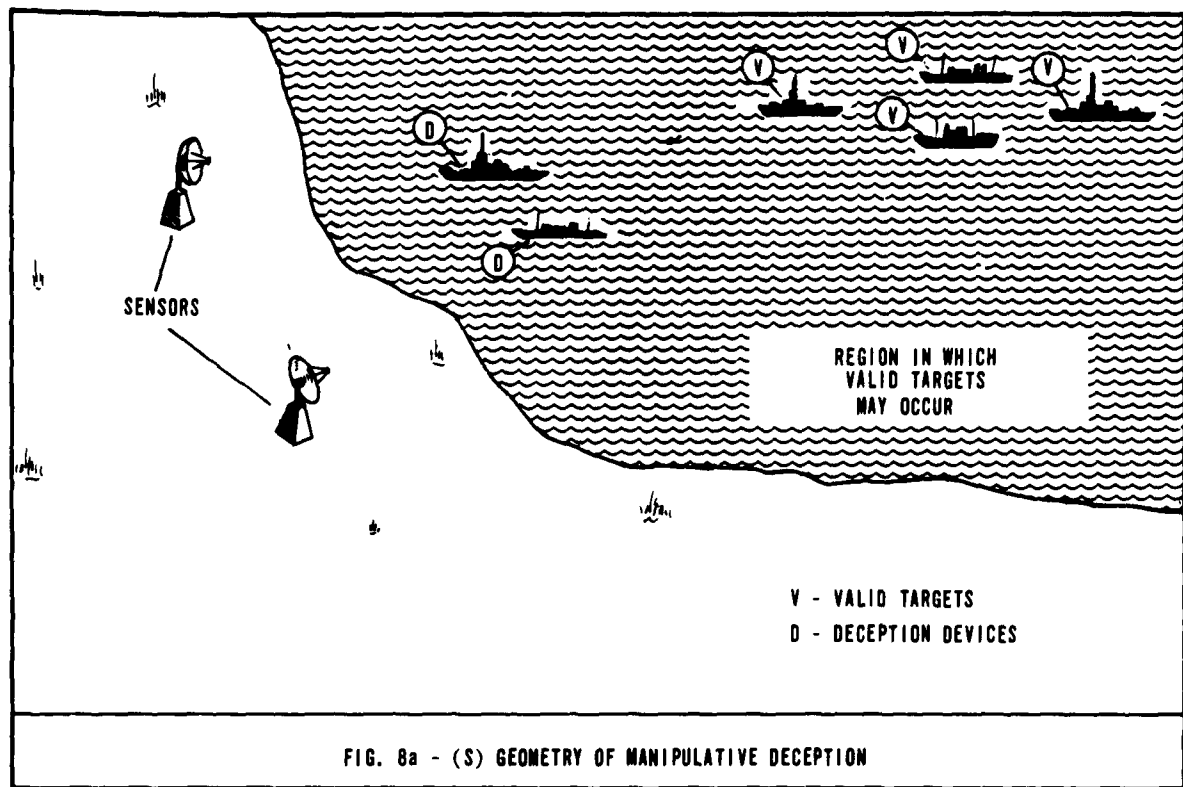
The techniques used against manipulative deception are in general different from those used in imitative deception. In the case of manipulative deception the enemy has at best a partially incomplete picture of friendly activities from which to estimate friendly capabilities and intentions. He must expect that even in the absence of manipulative deception he will receive somewhat conflicting indications, so that he cannot apply the test of accepting evidence of only perfectly logical and coherent activities in determining whether or not manipulative deception is being attempted. Further, since there is no cooperation between his units and the units he is observing, he has no direct means of authentication.

On the other hand, there exist some direct measures he can take against imitative deception. In this case he is "on his own territory." The basic patterns of operation of the unit which he is trying to recognize (his own communications transmitters) will be much more familiar to him than the patterns of operation of the assaulting forces which his intelligence system is trying to observe, and consequently deviations from his patterns of operation will be more noticeable and more meaningful. Further, he will normally be able to obtain cooperation with the friendly unit, and can use various direct authentication techniques.

The geometry of the situation also causes strong differences between the two cases (Figure 8). In the case of manipulative deception the deception device is usually located in a region where valid targets would be expected. From the enemy viewpoint, therefore, the location of the deception device does not in itself tend to identify it as a deception device (Figure 8a). (However if the enemy can resolve different deception devices this may unmask the deception in a way which will be discussed later. Gross location is being discussed at this point.)

In the case of imitative deception the valid target (his communication transmitter) is located in his territory, whereas the deception device will normally be located in our territory. Thus the location of the device tends to unmask its purpose, and he can take advantage of this fact by using techniques

SECRET



SECRET

which enable him to easily distinguish the direction of arrival of a signal (Figure 8b). Upon this basic geometrical truth rests much of the utility of lasers in anti-deception.

A. DETECTION OF DECEPTION OPERATIONS

From the enemy's standpoint the detection of a deception operation is essentially a problem in decision making, and the standard framework of classical hypothesis testing may shed some light on the process. The basic process in decision making involves the collection of information, the analysis of the collected data, and comparison of the results of the analysis with a threshold level ¹ (Figure 9). As an example, let us assume that the enemy has been monitoring friendly traffic for a period of time and is familiar with friendly radio procedure. Then in deciding whether or not new messages are from these familiar nets he would compare characteristics of the new messages with the original set. The characteristics chosen would be those which are stable for a given net over a period of time, but might be expected to vary between nets. Some of these characteristics are under conscious control of the net; others are generally uncontrolled. Examples of controlled variables are station call sign, net frequency (nominal), net schedule, and formatting of externals. Uncontrolled variables include such items as operator "fist," operator voice quality, and frequency drift. Some of the comparisons between the new message and the old traffic from the suspect net would be made on the basis of measured data, such as nominal frequency and drift characteristics of the transmitters. Some of the comparisons would be subjective, based upon the operator's ability to remember and compare patterns in such fields as operator fist. In the time period 1975 to 1980 many of the comparisons which are made manually today may be made automatically since it is reasonable to expect that the field of radio fingerprinting will make rapid strides in the next few years.

Slight deviations from the expected pattern will not normally signify a deception effort. Unusual deviations might do so. In order for the enemy analyst to decide what constituted a "slight" or normal deviation from an unusual deviation, it is necessary for him to have developed an estimate of

¹In statistical terms the statistic is examined to determine whether or not it falls in the critical region.

GENERAL	SPECIFIC EXAMPLE
COLLECT INFORMATION	COLLECT HISTORICAL DATA ABOUT OPERATING PROCEDURES INTERCEPT MESSAGE TO BE EXAMINED
ANALYZE COLLECTED DATA	WHAT IS THE PROBABILITY THAT A VALID SIGNAL ASSOCIATED WITH AN AMPHIBIOUS LANDING OPERATION WOULD HAVE THE OBSERVED FREQUENCY, CALL SIGN, OPERATOR CHARACTERISTICS, ETC. ?
COMPARE WITH THRESHOLD	IS THIS ENOUGH EVIDENCE TO REQUIRE THAT MILITARY PRE- PARATIONS BE MADE TO COUNTER THE THREAT?
FIG. 9 - (U) TESTING FOR A DECEPTION OPERATION	

what constitutes normal operations, and this must be based upon many observations. For instance, it may have been observed that call signs on the net are changed once a week at 1200 Z. Under these circumstances the enemy intelligence officer would be suspicious if the call sign were not changed at this time. In this case (because of previous patterns of operation) the lack of a change is more suspicious than a change would be.

To sum up, if the enemy has obtained enough data from observations of past operations so that he has been able to build up a picture of the range of variation that constitutes normal operations, then he has the means to estimate how unusual the new observation is. At this point he is almost ready to answer the question: "Is this the type of indication I would expect from a unit which was about to perform a [specific operation] or is it a deception operation?" He lacks only the estimate of the cost of making the two standard types of errors: (1) deciding that it is a deception operation when it isn't, or (2) deciding it is not a deception operation when it is. Exactly where the threshold will be set in determining that it is a deception operation depends heavily upon the specific tactical situation. For instance, if the indications he receives are that a landing force is heading for a probable landing point near a vital and unprotected rail center, then if he erroneously decides that it is a deception effort the cost to him will be very large. Under these circumstances if he has any troops to spare he will probably reinforce the defenses at the suspected landing area even if the evidence he receives is not overwhelmingly convincing. On the other hand, if he feels that the forces in being at the suspected landing area are sufficient to cope with probable landing forces, at least until reinforcements can be brought in, then he will probably insist that the evidence of an attack be very firm and convincing before he uses it to make any change in his deployments.

With this basic decision-making process in mind we see that there are three basic ways in which the enemy may increase his ability to discriminate against deception operations: (1) He may attempt to increase the amount of information he has about the opposing forces; (2) he may reanalyze the information already available to him; or (3) he may change his decision threshold, that is, insist that the evidence of an operation be very strong before he accepts it. The following discussion presents specific anti-deception techniques that may be used in each of these areas.

1. The Obtaining of New Information

This is the most powerful of the anti-deception approaches. Frequently one additional piece of information is enough to unmask the whole deception plan.

Two types of additional information may be obtained. It is possible to alter the operation or characteristics of the existing sensors so as to obtain more information of the type already available, or it is possible to use additional sensors to obtain new types of information.

As an example of alteration of the operation of existing sensors, consider the case when a communications intelligence intercept position discovers traffic on a net it is assigned to monitor. This information may then be used to direct the search of other intercept positions if past patterns of activity have been discovered. Information should be available about traffic which would likely be correlated on other nets, and the intercept coverage on these net frequencies may be increased. In this manner the probability of detecting confirming data if it exists may be increased, and alternatively the possibility of detecting the lack of expected confirming data is also increased.

When a communications intelligence search position detects suspect traffic this information may be used to direct DF stations. The DF stations then may obtain the location information which will enable geometric patterns of the suspect operation to be examined. This introduces a whole new element into the deception operation. Frequency and operating patterns of a large number of nets may be simulated by a few transmitters collocated aboard one ship; if the location of the ship is measured then any discrepancy between the operation implied by its location and the operation implied by the net traffic may be unmasked.

The capability to achieve higher resolution between transmitters will provide an even better anti-deception capability. In many phases of the amphibious operation ships would normally be expected to be dispersed by distances of five to fifty miles. An accurate DF capability, of the type which should be achievable even as low as HF in the 1975 to 1980 time frame, would enable these ships to be resolved. Under these conditions if the deception operation attempted to simulate a large number of ships and their associated net elements by placing a large number of transmitters aboard one ship, the

deception might quickly be unmasked. The introduction of a high-resolution DF capability would require that the geometry as well as the traffic patterns of the communications deception plan be realistic. Further, if the geometry of the traffic were cross-correlated with the time patterns of the traffic it is possible that a deception might be unmasked. For instance, if two elements of a net which were apparently in communication did not have the proper time spacing between elements of the message (such as both elements transmitting simultaneously in a simplex link) the message would immediately be seen to be a deception operation. Thus by using collection and analysis equipment capable of displaying the geometry of the transmitting elements and correlating it with all other information received, the enemy could unmask anything less than a very sophisticated deception operation.

The enemy may also use other types of sensors such as IR or photo, to collect new information about the situation. Thus if the communication traffic indicates that there are five ships communicating with one another and the IR sensors indicate only one, then the communications deception plan would be unmasked. This multi-sensor approach, which has been gaining steadily in usage during the early 1960's will be well developed by 1975 to 1980, and will provide a powerful discriminant against a deception operation.

The range and continuity of coverage of reconnaissance systems will be much larger in the period 1975 to 1980 than today because of the use of reconnaissance satellites, probably carrying multi-sensors. Because of this it will be very difficult to conceal the movement of large numbers of surface ships. By maintaining continuous files of the known locations of surface ships the enemy will be able to detect the initiation of a deception operation such as the simulation of a convoy unless the simulation were carried out from the points of embarkation.

2. The Reanalysis of Existing Information

Frequently the key to an enemy operation may be contained in existing data, but because of failure to ask the proper question, to look at the data in the proper light, or to rearrange it in the proper format it may go undiscovered. During the 1950's the art of collecting information far surpassed the art of analyzing it. During the 1960's the increased usage of automatic processing equipment has begun to remedy this situation. In the

1970's the use of automatic processing equipment, perhaps of a self-organizing type, will help to provide means of extracting almost all of the intelligence that is contained in a set of data. This capability of rapidly correlating data from different sensors is what makes the multi-sensor technique such a powerful discriminant against deception; a set of isolated deception plays aimed at each sensor individually would fail when the outputs of these sensors are properly correlated.

3. The Changing of the Decision Threshold

The enemy will have a high decision threshold (that is, act on the data only when it appears to have a high reliability) when:

- a. He suspects that deception operations are being conducted against him;
- b. To act on the data would radically weaken his capability to counter other threats if they should develop.

Conversely, he will tend to use a lower threshold (accept a hypothesis on the basis of less convincing evidence) if:

- a. He is not seriously considering the possibility that deception will be practiced against him;
- b. Acting on the basis of the information will not appear to greatly diminish his capability to cope with other threats that might appear.

Changing the decision threshold is not a very satisfactory method of discriminating against deception. If care is already being employed then the decision threshold may be raised only at the expense of decreasing the probability that valid information will be accepted. In other words, if they insist upon making decisions only when they are supported by overwhelming evidence, then they run a severe risk of refusing to take action against threats until it is too late. Conversely, one of the objectives of a deception effort is to cause this effect to take place; that is, to cause the enemy to mistrust his information enough that he will not accept valid information that he may have.

B. ENEMY ANTI-MANIPULATIVE DECEPTION OPERATIONS

The total effect of the enemy's increased capability to collect, store, analyze, and evaluate intelligence information will be to greatly increase the probability that incomplete (i. e., single-sensor oriented) deception operations will be uncovered in a short time. However, if the deception operation is very carefully controlled, and the enemy's low flying aircraft are denied access to the area, then deception operations in which a separate deception force is created may cause confusion as to which of two forces is the real one, even though it can quickly be determined that one is false. It is possible that the time required for the enemy to make a proper distinction between a real and deceptive action would be great enough to materially affect his capability to take counteraction. This will be true only if the Navy's policy of increasing mobility is vigorously pursued, for it is the relationship between the tempo of the enemy's decision making process and the tempo of the battle which is significant.

During this time period a sophisticated foreign power (the Soviet Union, France, Great Britain, Germany, or some other power) capable of launching and maintaining reconnaissance satellites will be able to detect the presence of any naval force sufficiently large to conduct a successful landing operation in the face of determined resistance. Denial operations aimed at preventing the enemy from detecting the presence of such a force will have a low probability of success. Denial operations must, therefore, be aimed at preventing the intent of such a force from being disclosed. Countries which do not have access to information collected by such satellites may not be able to track such a task force under all weather conditions. It will be entirely possible to deny any country communications intelligence incident to the movement of such a task force. Communications may be made secure by such means as lasers for communications between elements of the task force and by secured links from satellite relays for communications between the task force and its base of operations.

Some of the methods and techniques which will be available to the enemy to aid him in his attempts at deception resistance include:

1. Almost continuous surveillance of world-wide military operations.
2. Precision radio location finding techniques.
3. Precision fingerprinting techniques to assess each threat as real or deceptive.
4. Multiple sensor systems which include proper time correlation within each sample taken.
5. High speed collection, evaluation, and real time presentation of intelligence information.

C. ENEMY ANTI-IMITATIVE DECEPTION OPERATIONS

The ultimate factor in determining the success of an imitative deceptive effort is dependent upon how loosely the enemy operators conduct their operations and how gullible they may be to psychologically oriented suggestions. It appears then that those techniques which minimize or, if possible, prevent conditions of this nature from existing would certainly build the enemy's resistance to imitative deception. A number of techniques are currently in use and others will find application in future operations. A list of this nature may include:

1. Voice recognition techniques
2. Regular use of authentication procedures
3. Burst communication techniques
4. Frequency shifting procedures
5. Cryptographic methods
6. Intense training of operators to resist psychological intrusion.

D. U. S. EFFORT TO OVERCOME ANTI-DECEPTION OPERATIONS

As the enemy's ability to obtain a geometric picture of the deployment of ships, from the associated communications traffic, increases it will become more necessary to realistically deploy the deception transmitters. During the time period 1975 to 1980 it will be possible to deploy these transmitters realistically and relatively inexpensively by utilizing small ships to simulate larger ones. However, this effort will be discovered quickly if the enemy can use sensors which are capable of determining the size of the ship. For this reason deception operations on a large scale are possible against a sophisticated enemy only if they are carried out in conjunction with systematic destruction or neutralization of enemy sensor systems in satellites or aircraft, or if some means can be devised to mask these operations from the sophisticated sensors. If such operations can be conducted, then it should be economically feasible to complete the deception against the remaining sensors and, in particular, the enemy's communications intelligence system.

Short-term, localized deception about the location, direction, and intent of a naval force may be conducted even in the presence of satellite- and aircraft-borne sensors if localized fogs can be created. The current research in this area should be continued. If a fog, or other atmospheric suspension of particles which absorb or scatter visible and infrared radiation, can be created over the region in which the deception is to take place then those sensors which can recognize the size and shape of ships will be negated, and the deception against radar, ELINT, communications intelligence and acoustical sensors can be carried out cheaply by a deployment of energy sources on small ships which are capable of presenting the geometric deployment pattern of a large force.

Efforts should be made to locate and destroy the enemy's analysis centers. Manual analysis, scattered over many points, will not be able to efficiently utilize all the information which a fully operating set of sensors could collect. Only by utilizing centralized computational facilities, which then become lucrative targets, can the enemy maintain the real-time picture of operations which is envisioned here. If these facilities can be partially or completely denied to him, then deception operations become feasible which otherwise would be unsuccessful.

VI. ENEMY DECEPTION THREAT

The ability of an enemy, in defense of a shoreline against an assault from the sea, to successfully employ techniques of deception against his adversaries could conceivably result in the assault force paying a much higher price, in men and material, for that beachhead than was originally estimated. To increase the probability of being successfully deceptive, however, his deception tactics must be practiced on a continuous basis, as an integral part of his defense. It is as important, therefore, for him to work at confusion of his adversary's pre-invasion reconnaissance efforts as it is to attempt to insert confusion into the assault force operation while it is actually taking place.

The enemy of 1975-1980 will be aware of the sophisticated surveillance tactics on the part of his potential attacker, who will be employing the multiple sensor concept of simultaneous photographic (including TV), infrared, visual, radar, and possibly ELINT surveillance from a single platform. He can expect this type of reconnaissance from ships, both surface and sub-surface, and from aerospace vehicles, including low-flying drones, manned aircraft, and manned and unmanned spacecraft. The purpose of these missions, both prior to and during an assault, will be, of course, to assess his apparent positions of strength and weakness. The validity of the data accumulated by these surveillance vehicles will be of inverse proportion to his ability to deceive.

High resolution aerial photography (better than 200 lines/mm) will use color film in place of the now-standard black-and-white by this time period. This type of film has the advantage of being able to display the difference between natural foliage and that which was cut for use as camouflage. Knowing this, the enemy can be expected to utilize more natural cover for camouflage. Where this scheme is not practical, synthetic materials will be used, with color contents very similar to the natural. In an attempt to deceive those who are surveying him, however, the enemy can also be expected to decoy the color camera with detectable camouflage over false emplacements, creating positions of men and/or materiel that do not exist.

The use of low fidelity decoys, such as pre-fabricated pneumatic devices, will be more prevalent in the 1975-1980 time period. These are inflatable objects, simulating artillery pieces, wheeled vehicles, and tanks, which, from a proximity of 1000 feet or more, create a very realistic image. They

can be covered with materials that will provide authentic returns to radar and thermal sensors. These devices will be used to decoy tactical surveillance and subsequent bombardment away from the actual gun and missile emplacements. They can be dismantled, moved, and erected in a few hours, providing a mobile technique of deception that can be highly effective.

The entrenched shoreline defender will utilize subterranean emplacements, both natural and manmade, to the greatest degree possible. This provides excellent protection for men and weapons against surveillance and bombardment. Since the heat exhausting from the ventilation systems of these locations would be a giveaway to a thermal sensor, ducts will probably be constructed to carry the exhaust gases to a remote point, removed from the actual underground location. A decoy might be built around these ventilators that would indicate to both the thermal and photographic sensors that an emplacement exists at that point.

Since the Soviets have been concentrating research effort on aids to night driving, such as active infrared periscopes and binoculars, it can be expected that movement of vehicles in the defense area will take place mainly under the cover of darkness. Speeds in excess of 20 mph have been attained with no visible illumination. These vehicles will also be equipped with heat shields over their engines, another Soviet experiment, to mask the "hot spot" created by the running engine. This ruse has worked against present infrared surveillance systems with a reasonable degree of success.

The vehicle parking area will probably be heavily covered by natural foliage or painted tarpaulins that look, to the color camera, somewhat natural. It is difficult at this time to predict the degree to which aerial color photography can be duped by artificial camouflage; however, it is expected that countermeasure research will continue on synthetics to be used against this type of surveillance. The cover over the parking area will eventually warm up to a point where it is detectable by a thermal sensor, because of the activity beneath, however, the type and quantity of vehicles parked there cannot be detected.

In an attempt to decoy thermal sensors away from actual emplacements of weapons, vehicles, and troops, devices such as flare pots, electric heaters, and "canned" heaters have been used with some success. In the future, devices such as the GaAs diode, with improved efficiency, could be used as an infrared emitter

decoy in a strategic situation. Entire nets of these devices could be laid, similar to a communications network, whose characteristics could be changed electronically to simulate changing conditions on the ground. This tactic would relieve squads of personnel from the task of lighting and scattering flare pots, heaters, etc., in attempting the same type of deception.

These tactics would be only a temporary confusion factor, however, since the concept of multiple sensor surveillance would eventually separate the actual from the decoy. For example, the combination of night driving aids plus heat shielding might make a convoy of vehicles undetectable by infrared surveillance, but a thermal system backed up by a high resolution MTI radar would not be fooled. In a recent Project MICHIGAN report it was stated,¹

"--- The mobility capabilities of both the Soviet and U. S. Army provide the means to group and move significant forces long distances overnight or during brief inclement weather. The U. S. has felt it urgent to develop a means to detect enemy motion during these periods when optical sensors, and to a large extent IR sensors, are of little help. The selection was MTI radar. "

The enemy, aware of the importance placed by the U. S. on this technique, can therefore be expected to attempt deception or confusion jamming or a combination thereof, on MTI radar surveillance in conjunction with their efforts to deceive the photo and thermal sensors. Present MTI radars operate at X-band and utilize the pulsed Doppler method of target detection, displaying relative movement between target and ground clutter. An aural output is presented to the operator allowing recognition and distinction between wheeled vehicles, tracked vehicles, and walking personnel. To deceive an MTI radar of this type, it is necessary for the jammer to radiate signals which are of the same nature as the radar returns from actual targets. The RF will be similar to the victim radar's frequency and the energy contained in the pulses from the jammer will be of levels typical of the simulated targets. These pulses will be modulated with Doppler simulations of wheeled vehicles,

¹J. Armstrong/J. Gautt/J. Maddus, Sylvania Electronics Systems, 9th Annual Radar Symposium Record.

tracked vehicles, walking personnel, or a combination of these. The jamming equipment necessary to provide the confusion, or deception, jamming just described against battlefield surveillance will be portable enough to be carried by a man, thereby giving extreme mobility to the jammer. To provide the power necessary to perform against surveillance aircraft, either manned or drones, the jammer will be mounted on a vehicle along with the required power generators. The CHEESE BRICK equipment, with its associated MERCURY NOSEBAND truck, is an example of an X-band system, possibly capable of jamming an MTI radar.

Three types of jamming, spot, broadband, and deceptive jamming, may be used with various degrees of effectiveness against noncommunications targets. Figure 10 summarizes the requirements that these types of jammers must meet in order to be effective against some of the newer and forthcoming types of noncommunications equipments. A summary of the basic characteristics of some known noncommunications jammers in use by the Soviets is contained in Figure 11.

Techniques of radar deception, such as the use of corner reflectors, will probably still be in evidence in this time period. These devices, which are metallic objects formed in three mutually perpendicular planes, simulate ground targets, such as vehicles, by returning an echo to the surveillance radar that is similar to that normally returned from a larger target. This type of decoy, like the flare pot and electric heater used against the infrared sensor, is of limited value in a tactical situation because of the concentration of interest by the data analyst on relative movement of the target.

At the present time, research is underway in the Soviet Union and its satellites on radar absorbent materials. The use of dielectrics, magnetic material, and glass fiber reinforced fabric is being investigated for this purpose. Further work in this field may produce, by the 1975-1980 time period, missiles, aircraft, trucks, and tanks, coated with these absorbents in an effort to deceive surveillance and tracking radars.

In a further attempt to confuse the radar sensor, the Soviets can be expected to utilize "chaff" dispensing rockets. These devices may be launched from aircraft or from the ground.

SECRET

JAMMER TYPE	RADIATOR TYPE	MODULATION TYPE REQUIRED	LOOK-THRU REQUIRED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	
SPOT	CONVENTIONAL PULSED RADAR	NOISE, PULSE, OR COMBINATION	YES	JAMMER POWER AT LEAST 3 db ABOVE SIGNAL POWER AT TARGET RECEIVER FOR PULSE JAMMING.	BANDWIDTH OF EMITTER PLUS ALLOWANCE FOR MAGNETRON DRIFT	MANUAL OR AUTO TUNED	V K N C
	JUMP FREQUENCY RADAR	NOISE, PULSE, OR COMBINATION	YES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OVER WHICH FREQUENCY OF RADAR VARIES	MANUAL OR AUTO TUNED	V K N C
	PULSE CODED RADAR	NOISE, PULSE OR COMBINATION	YES*	JAMMER POWER AT LEAST 3 db ABOVE SIGNAL POWER AT TARGET RECEIVER FOR PULSE JAMMING.	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	V K N C
	PULSE DOPPLER	NOISE, PULSE, OR COMBINATION	YES	3 db OR MORE OVER TARGET RETURN	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	V K N C
	PULSE COMPRESSION RADAR	NOISE, PULSE, OR COMBINATION	YES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	EXTREMELY RAPID TUNING WITHIN PULSES	V K N C
	NAV. AID BEACONS	NOISE, POSSIBLY PULSE, OR NOISE PULSE COMBINATIONS	YES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET NAV. AID TRANSMITTER	MANUAL OR AUTO TUNED	V K N C
	IR GUN DIRECTORS	NOISE	YES*	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	IR HIG FIL APP RAN
BROADBAND	CONVENTIONAL PULSED, PULSE CODED, PULSE DOPPLER, PULSE COMPRESSION	NOISE, PULSE, OR COMBINATION	NO	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	MANUAL	V K N C
	JUMP FREQUENCY RADAR	NOISE, PULSE, OR COMBINATION	YES	AT LEAST 3 db OVER SIGNAL AT TARGET SIGNAL	BANDWIDTH OVER WHICH TARGET RADAR VARIES	SWEEPING AT SWEEP RATE GREATER THAN PRF OF TARGET RADAR	V K N C

1

FIG. 10 JAMMER REQUIREMENTS FOR NONCOMMUNICATIONS TARGETS

SECRET

SECRET

LOOK-THRU MODE	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	POWER TUBE TYPE REQUIREMENTS	RECEIVER TYPE REQUIRED	REMARKS
S	JAMMER POWER AT LEAST 3 db ABOVE SIGNAL POWER AT TARGET RECEIVER FOR PULSE JAMMING.	BANDWIDTH OF EMITTER PLUS ALLOWANCE FOR MAGNETRON DRIFT	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	CRYSTAL VIDEO OR SUPER- HETERODYNE	SPOT JAMMER VERY EFFECTIVE IF IT TRANSMITS PULSES DURING PULSE INTERVALS OF EMITTER
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OVER WHICH FREQUENCY OF RADAR VARIES	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	WIDEBAND CRYSTAL VIDEO OR POSSI- BILITY RAPID SCAN	SWEEPING RECEIVER (VERY RAPID SWEEP) MAY BE USEFUL, THOUGH WIDE-OPEN RECEIVER MORE DESIRABLE
	JAMMER POWER AT LEAST 3 db ABOVE SIGNAL POWER AT TARGET RECEIVER FOR PULSE JAMMING.	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	CRYSTAL VIDEO OR SUPER- HETERODYNE	PULSE JAMMERS VERY EFFECTIVE. *LOCK-ON CAPABILITY FOR RAPIDLY CHANGING CODES NECESSARY
	3 db OR MORE OVER TARGET RETURN	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	VOLTAGE TUNED CARCINOTRON	WIDEBAND CRYSTAL VIDEO OR POSSI- BILITY RAPID SCAN	RADIO FREQUENCY CHANGES OF RADAR DETERMINED BY KNOWN VELOCITY RANGE OF ITS TARGETS
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	EXTREMELY RAPID TUNING WITHIN PULSES	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	CRYSTAL VIDEO OR SUPER- HETERODYNE	
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET NAV. AID TRANSMITTER	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	SUPERHETERODYNE	JAMMING REQUIREMENTS FOR U S TACAN NOT KNOWN
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	MANUAL OR AUTO TUNED	IR NOISE SOURCE WITH HIGH POWER CAPABILITY; FILTERS TO COVER APPROPRIATE WAVELENGTH RANGE	BROADBAND IR DETECTORS (APPROX 1 MICRON TO 50 MICRONS AT PRE- SENT)	*THE LOOK-THRU SHOULD PERMIT DETERMINATION OF BANDWIDTH OF TARGET TRANSMITTER. REQUIRED JAMMER BW WILL THEN BE EQUAL TO THAT OF TARGET TRANSMITTER
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVER	MANUAL	VOLTAGE TUNED KLYSTRONS, MAG- NETRONS, OR CAR- CINOTRONS	CRYSTAL VIDEO OR SUPER- HETERODYNE	SPECIAL CASE OF ABOVE DESCRIPTION OF SPOT JAMMING INCREASED POWER OVER SPOT JAMMING REQUIREMENT NECESSARY FOR EFFECTIVENESS
	AT LEAST 3 db OVER SIGNAL AT TARGET SIGNAL	BANDWIDTH OVER WHICH TARGET RADAR VARIES	SWEEPING AT SWEEP RATE GREATER THAN PRF OF TARGET RADAR	VOLTAGE TUNED KLYSTRONS MAG- NETRONS, OR CAR- CINOTRONS	CRYSTAL VIDEO OR VERY WIDEBAND SUPERHETERODYNE	

FIG. 10 JAMMER REQUIREMENTS FOR NONCOMMUNICATIONS TARGETS

SECRET

SECRET

JAMMER TYPE	RADIATOR TYPE	MODULATION TYPE REQUIRED	LOOK-THRU REQUIRED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	
BROADBAND (CONTINUED)	MILLIMETER WAVE RADAR	NOISE PULSE, OR COMBINATION	YES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVERS	MANUAL OR AUTO TUNED	PON CAP MIL OPE
	IR GUN DIRECTORS, IR SURVEILLANCE	NOISE	YES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVERS	MANUAL OR AUTO TUNED	HIGH SQUI
DECEPTIVE	CONVENTIONAL PULSE PULSE CODED, PULSE DOPPLER, PULSE COMPRESSION	PULSED	NO	TO SEVERAL HUNDRED WATTS	BW OF RADAR BEING "CAPTURED"	MANUAL OR AUTO TUNED	VOLT STRO OR C
	JUMP FREQUENCY RADAR	PULSED	NO	TO SEVERAL HUNDRED WATTS	BW OF RADAR TO BE IMITATED	ELECTRICALLY TUNED TO FREQUENCY OF LAST PULSE RECEIVED	VOLT, STRO OR C
	MILLIMETER WAVELENGTH RADAR	PULSED PULSE CODED, ETC	NO	TO SEVERAL HUNDRED WATTS	BW OF RADAR TO BE IMITATED	MANUAL OR AUTO TUNED	VOLTA STRO OR CA
	IR GUN DIRECTORS AND SURVEILLANCE DEVICES	NOT APPLICABLE	NO	DEPENDS UPON TARGET TO BE SIMULATED	NOT APPLICABLE	NOT APPLICABLE	IR SOI POWER BLY EI PANELS PERSON

FIG 10 - JAMMER REQUIREMENTS FOR NONCOMMUNICATIONS TARGETS (CON)

1

SECRET

SECRET

THRU RED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	POWER TUBE TYPE REQUIREMENTS	RECEIVER TYPE REQUIRED	REMARKS
ES	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVERS	MANUAL OR AUTO TUNED	POWER OUTPUT TUBE CAPABLE OF FUNDAMENTAL MILLIMETER WAVE OPERATION	CRYSTAL VIDEO OR SWEEP SUPERHETERO- DYNE	FOR SOME PRESENTLY KNOWN MM WAVE POWER TUBE CAPABILITIES, SEC SECTION 251
	AT LEAST 3 db OVER SIGNAL AT TARGET RECEIVER	BANDWIDTH OF TARGET RECEIVERS	MANUAL OR AUTO TUNED	HIGH POWER IR NOISE SOURCE	WIDEBAND IR RECEIVER	RECEIVER REQUIRED
	TO SEVERAL HUNDRED WATTS	BW OF RADAR BEING "CAPTURED"	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLY- STRONS, MAGNETRONS, OR CARCINOTRONS	CRYSTAL VIDEO OR SWEEP SUPER- HETERODYNE	REPEATER JAMMER AMPLIFIES "CAPTURED" PULSES 3 db OR MORE AND RETURNS THEM TO TARGET DELAYED IN TIME. FOR PULSE DOPPLER, RADAR PULSE SHAPE MUST NOT BE DISTORTED FOR EFFECTIVE DECEPTION.
	TO SEVERAL HUNDRED WATTS	BW OF RADAR TO BE IMITATED	ELECTRICALLY TUNED TO RE- QUENCY OF LAST PULSE RECEIVED	VOLTAGE TUNED KLY- STRONS, MAGNETRONS, OR CARCINOTRONS	NONE	DEVICE WOULD BE USEFUL AGAINST ELINT EW INTERCEPT OPERATIONS POSSIBLY REMOTELY CONTROLLED BY RADIO SHOULD SIMULATE SCAN- NING FUNCTIONS
	TO SEVERAL HUNDRED WATTS	BW OF RADAR TO BE IMITATED	MANUAL OR AUTO TUNED	VOLTAGE TUNED KLY- STRONS, MAGNETRONS, OR CARCINOTRONS	NONE	DEVICE WOULD BE USEFUL AGAINST ELINT EW INTERCEPT OPERATIONS POSSIBLY REMOTELY CONTROLLED BY RADIO SHOULD SIMULATE SCAN- NING FUNCTIONS.
	DEPENDS UPON TARGET TO BE SIMULATED	NOT APPLICABLE	NOT APPLICABLE	IR SOURCE OF HIGH POWER OUTPUT (POSSI- BLY ELECTROLUMINESCENT PANELS TO SIMULATE PERSONNEL OR VEHICLES)	NOT APPLICABLE	DECEPTIVE USE OF DEVICES TO SIMULATE SUCH FUNCTIONS DEPENDS UPON WHETHER THESE FUNCTIONS ARE CARRIED OUT USING ACTIVE OR PASSIVE IR

FIG 10 - JAMMER REQUIREMENTS FOR NONCOMMUNICATIONS TARGETS (CONT'D)

2

SECRET

FREQUENCY RANGE	NOMENCLATURE	POWER OUTPUT	MODULATION TYPE	BANDWIDTH	MOBILITY	PURPOSE	REMARKS
11.1-16.6 Mc ¹	1-VF	4 kw	UNK	UNK	UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
86-200 Mc ²	PR-158*	80-200W	WHITE NOISE	UNK	AIRBORNE	JAMMER	1 AIRPLANE REQUIRED PER JAMMER
2000-3000 Mc ¹	UNK	300W (AVERAGE) 3kw (PEAK)	PULSE	UNK	UNK	JAMMER	
2300-3750 Mc ²	PR-150*	80-200W	WHITE NOISE	UNK	AIRBORNE	JAMMER	1 AIRPLANE REQUIRED PER JAMMER
2000-15,000 Mc ¹	UNK	UNK	UNK	UNK	UNK	JAMMER	
2000-15,000 Mc ²	UNK	UNK	UNK	UNK	UNK	JAMMER	TYPE OF JAMMER NOT SPECIFIED BY SOURCE. MAY BE RADAR JAMMER
8572-10,345 Mc ²	SPB-1 (CHEESE BRICK)	160W (CW)	55-60% AM	UNK	MOBILE	INTERCEPT AND JAMMING	TRANSPORTED IN GAZ-63 VEHICLE
15.5-17 kmc ³	UNK	60W	NOISE	5 Mc	MOBILE	JAMMING	THIS K _U -BAND JAMMER NOT OPERATIONAL. DEVELOPMENT IS EXPECTED ABOUT 1961-1962

1. US ARMY SIGNAL RESEARCH AND DEVELOPMENT LABORATOR, FORT MONMOUTH; S4574-58, 8 OCTOBER 1958; SECRET/NOFORN.

2. CIA, CS-K-3/352, 502, SOVIET ELECTRONICS EQUIPMENT, 21 APRIL 1958; SECRET/NOFORN/CONTINUED CONTROL.

3. NOHAD, WEEKLY INTELLIGENCE REVIEW 17-60, 29 APRIL 1960; SECRET/NOFORN.

* DIRECT EVIDENCE REVEALS JAMMERS IN THE B AND D SECTIONS OF THE PR-15 SYSTEM ONLY. ACCORDING TO THE SOURCE OF INFORMATION,² IN CASE OF DANGER OR TRACKING BY AAA RADARS DURING SIGNAL INTERCEPT MISSIONS, EITHER OR BOTH JAMMERS ARE ACTIVATED TO SCREEN THE ENTIRE FLIGHT OF FIVE TU-4 AIRCRAFT COMPRISING THE PR-15 SYSTEM. HOWEVER, THE SOVIETS MUST BE AWARE OF THE POSSIBILITY OF ILLUMINATION BY RADARS OPERATING OUTSIDE THE FREQUENCY RANGES OF THE B AND D JAMMERS. IT IS THEREFORE CONJECTURED THAT THE A, V, AND G SECTIONS HAVE SIMILAR JAMMING EQUIPMENTS WITH FREQUENCY RANGES OF 60-86 Mc, 214-600 Mc, AND 1000-2000 Mc, RESPECTIVELY.

FIG. 11 - (S/NOFORN) SOVIET NONCOMMUNICATIONS JAMMERS

SECRET

The enemy will be cognizant, in this time period, of attempts on the part of his adversary to extract intelligence information, prior to, and during, an assault, from his communications networks. Since the positions of the defenders will be spread over long distances of shoreline, his phone lines, and radio and TV transmissions will be vulnerable to COMINT techniques such as line tapping by BJU's on-shore agents, and communications monitoring devices, ground and/or airborne. The airborne listening devices may be one of the multiple sensors in a surveillance manned aircraft or drone. Remote transponders may be dropped adjacent to enemy positions to accomplish the same purpose. These tactics on the part of his adversary will force the enemy to resort to deception tactics as a counter-measure.

In this situation the entrenched defender has the advantage of utilizing equipments that may be large, complex, and power consuming, because of his somewhat permanent location. For example, he can be expected to use the technique of burst communication to hinder an unwanted listener. This scheme utilizes a multiple speed tape recorder on either end of a communications link, to compress the time of the senders message by prerecording it before transmission, and then, on the receiver's end, performing the conversation back down to real time clear text. Standard techniques of authentication and voice recognition can be an accessory to this scheme as well as any other type of communications where clear text is used.

The enemy can also be expected to use "scramblers" in his communications equipment, even down to the most portable "walkie-talkie." In this scheme, the sender's clear text is first sampled, or commutated, and the samples are then mixed prior to transmission. The decoding equipment is a part of the receiver, where the message is unscrambled to convert it to clear text. The deception capability of this technique is good, because of the many encoding, and decoding, combinations available, which can be changed automatically.

Because of the extreme difficulty in determining the presence of a communications signal within a band of noise, the enemy's use of a noise communications system would present a major problem to an ECM unit. If a noncoherent noise system is used, problems for an EW effort are greatly magnified, because of the time and equipment needed by the intercept group to gather intelligence data from

SECRET

this type of system. Broadband jamming of a noise communications system seems theoretically most effective at this time; however, the power required to jam is probably greater than that tactically practicable for an amphibious assault force.

The future development of the laser will provide a battlefield commander, holding a fixed position, with the capability of communication with his units, with little danger of an intelligence leak. Since the laser is an optical system it is limited to line-of-sight operation, with the further inherent problem of difficulty in beam interception. However, the shoreline defender again has an advantage in utilizing this type of communications link because of his operating from a fixed position with adequate available power and time to set up his laser systems, which then remain fixed. The system would be almost undetectable to anyone not within a thousand yard radius of the beam receiver, making it an excellent device for communication of audio and video in the enemy positions immediately behind the forward area.

During an actual assault on this position, the enemy can be expected to attempt to insert a confusion factor into the assault operation by interfering with the operation of his attacker's communications nets. If his intention is to continuously jam the communications of the assault force, his fixed position is in his favor because of the available power at his disposal. He may use the "capture" technique of high-level transmission of an FM modulated carrier that is close to the frequency used by the net to be jammed, thereby overriding the legitimate signal with the jamming signal, and providing the receiver operator with the jamming tone, rather than the expected intelligence. This type of jamming could be keyed to the opposing transmitter in such a fashion that the jammer is activated only when a transmission is taking place. Unless the sender is monitoring his own transmission, he is then unaware of the attempt at jamming.

In general, three basic types of jamming can be distinguished:

1. Spot jamming entails the selective masking of an emitter's signals in a restricted bandwidth. Through this restriction a great deal of power may be focused on the receiver, ensuring jamming within that frequency range.

2. Broadband or barrage jamming implies the coverage of a relatively wide band of frequencies by the jammer either through complete continuous coverage of the emitter's total frequency range or through rapid sweeping of the band.
3. Deceptive jamming includes the insertion of false or misleading information into an enemy's receivers or changing the characteristics or parameters of the information being received.

Figure 12 summarizes the requirements that these three types of jamming must meet in order to be effective against some newer types of communications systems.

Deceptive jamming against data transmission systems, though difficult to accomplish, could be very effective in a tactical situation. The most likely type of communications deception to succeed during an assault operation, however, is either imitative or manipulative deception, or a combination thereof. Using the imitative deception tactic, the enemy would attempt to intrude into his adversaries' communications nets and insert false information for the purpose of confusing his attacker. This technique would be most successful during an amphibious assault because of: (1) the fast-moving tactical situation and (2) the lessening of communication security and discipline that is inherent in an operation of this type. If the enemy has capable operators and detailed information on the circuits used by the assault force, his application of this tactic could result in considerable confusion on the part of his attacker due to fictitious reports of troop movements, casualties, etc.

The enemy, practicing manipulative deception techniques, would utilize the transmission of erroneous information over his own communications networks in an attempt to mislead his opponent's traffic analysts. His purpose would be the creation of situations concerning troop or weapons movements, casualty reports, and tactical information, through "dummy" traffic, in a further attempt to gain tactical advantage via electronic deception.

Figure 13 summarizes characteristics of some known communications jamming equipments in use by the Soviet and Bloc countries. It should be noted that the 500 w FK-500 should be adequate, at the present time, to overpower most Western transmitters at their receivers in a tactical situation.

SECRET

JAMMER TYPE	RADIATOR TYPE	MODULATION TYPE REQUIRED	LOOK-THROUGH REQUIRED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	
SPOT	CONVENTIONAL RADIO AM	AM OR FM NOISE OR VARIOUS TONE MODULATION TECHNIQUES	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE AM TARGET RECEIVER	MANUAL AUTO TUNED, POSSIBLY REMOTE	FR TO WA SP
	CONVENTIONAL RADIO FM	FM NOISE OR VARIOUS TONE MODULATION TECHNIQUES	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE FM TARGET RECEIVER	MANUAL AUTO TUNED, POSSIBLY REMOTE	FR TO WA SP
	DATA TRANSMISSION	AM OR FM NOISE OR PULSE	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE TRANSMITTED INTELLIGENCE	MANUAL OR AUTO TUNED	FR TO WA SP
	NOISE TRANSMISSION	AM OR FM NOISE OR PULSE	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE TRANSMITTED INTELLIGENCE*	PROBABLY SCANNING (AUTO)	FR TO WA SPI
	SINGLE OR DOUBLE SIDEBAND	AM NOISE OR VARIOUS TONE MODULATION TECHNIQUES	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF TARGET RECEIVER (FOR DSB) IN GENERAL INFORMATION BW	MANUAL OR AUTOMATIC	FR TO WA
BROADBAND	CONVENTIONAL RADIO AM						
	CONVENTIONAL RADIO FM	FM NOISE OR VARIOUS TONE MODULATION TECHNIQUES	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	AT LEAST AS GREAT AS FM DEVIATION OF TARGET RECEIVER	MANUAL OR AUTO TUNED	FR TO WA SPE
	DATA TRANSMISSION						
	NOISE TRANSMISSION						

FIG 12 - (S) JAMMER REQUIREMENTS FOR COMMUNICATIONS TARGETS

1

SECRET

SECRET

POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	POWER TUBE TYPE REQUIRE- MENTS	RECEIVER TYPE REQUIRED	REMARKS
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE AM TARGET RECEIVER	MANUAL AUTO TUNED, POSSIBLY REMOTE	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS DEPENDING ON SPECIFIC SITUATIONS	AM CAPABILITY REQUIRED	SIMPLEST TYPE OF EQUIPMENT TO JAM
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE FM TARGET RECEIVER	MANUAL AUTO TUNED, POSSIBLY REMOTE	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS DEPENDING ON SPECIFIC SITUATIONS	FM CAPABILITY REQUIRED	PRIMARY REQUIREMENT IS HEAVY CONCENTRATION OF ENERGY OVER ENTIRE FM DEVIATION OF THE RF CARRIER
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE TRANS- MITTED INTELLI- GENCE	MANUAL OR AUTO TUNED	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS DEPENDING ON SPECIFIC SITUATIONS	PULSE SIGNAL RECEIVER	ERROR INSERTION MAY BE BEST METHOD OF JAMMING THEREFORE PULSE JAMMING MAY BE MOST DESIRABLE
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE TRANS- MITTED INTELLI- GENCE"	PROBABLY SCANNING (AUTO)	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS DEPENDING ON SPECIFIC SITUATIONS	WIDEBAND	"VARIOUS METHODS MAY BE EMPLOYED TO MODULATE THE CARRIER OF NOISE TRANSMISSION SYSTEMS IN ONE LIKELY METHOD THE INFORMATION BW IS VERY SMALL PER CENT OF THE TOTAL BW USED IN GENERAL SPOT JAMMERS WILL NOT BE USEFUL AGAINST NOISE TRANSMISSION BUT BROAD BAND JAMMERS WILL
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF TARGET RECEIVER (FOR DSB) IN GENERAL INFOR- MATION BW	MANUAL OR AUTO- MATIC	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS	NORMAL AM WITH BFO OR SSB DSB HIGH RF STABILITY REQUIRED	BROADBAND JAMMING IS APPLICABLE UNDER THE SAME CONDITIONS BUT HAS NO DISTINCT ADVANTAGE OVER SPOT JAMMING IN THIS CASE
					SPECIAL CASE OF ABOVE SPOT JAMMING (AM); BROADER BAND COVERAGE REQUIRED
AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	AT LEAST AS GREAT AS FM DEVIATION OF TARGET RECEIVER	MANUAL OR AUTO TUNED	FROM SEVERAL WATTS TO SEVERAL HUNDRED WATTS DEPENDING ON SPECIFIC SITUATIONS	FM CAPABILITY REQUIRED	SEE FM ABOVE
					SPECIAL CASE OF ABOVE SPOT JAMMING (DATA TRANSMISSION); BROADER BAND COVERAGE REQUIRED
					SPECIAL CASE OF ABOVE SPOT JAMMING (NOISE TRANSMISSION); BROADER BAND COVERAGE REQUIRED

FIG 12 - (S) JAMMER REQUIREMENTS FOR COMMUNICATIONS TARGETS

2

SECRET

SECRET

JAMMER TYPE	RADIATOR TYPE	MODULATION TYPE REQUIRED	LOOK-THROUGH REQUIRED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	T
BROADBAND (CONT D)	IR COMMUNICATIONS	AM OR FM NOISE	YES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE IR RECEIVER TO BE JAMMED	MANUAL OR AUTO TUNED	HIGH
	SINGLE OR DOUBLE SIDEBAND						
DESCRIPTION	CONVENTIONAL RADIO (SIGNAL INSERTION)	VOICE CW, CLEAR TEXT OR ENCIPHERED	YES	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL TUNING	HIGH WIDEB NORMA BAND PORTI
	DATA TRANSMISSION	PULSE	YES	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL OR AUTO TUNED	NOT S
	NOISE TRANSMISSION	FM NOISE	YES	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL TUNING	NOT S
	IR COMMUNICATIONS	VOICE CW PULSE	YES	UP TO SEVERAL WATTS	BW OF TARGET RECEIVER	MANUAL OR AUTO TUNED	IR SQ WATTS
	SINGLE SIDEBAND	VOICE CW, CLEAR TEXT OR ENCIPHERED	YES	AT LEAST AS GREAT AS SIGNAL POWER AT TARGET RECEIVER AND PREFERABLY GREATER	BW OF TARGET RECEIVER	MANUAL TUNING	HIGH SELEC BAND

FIG 12 (S) JAMMER REQUIREMENTS FOR COMMUNICATIONS TARGETS (CONT D)

1

SECRET

SECRET

OK - OUGH IRED	POWER OUTPUT REQUIREMENTS	BANDWIDTH REQUIRED	TUNING CAPABILITY REQUIRED	POWER TUBE TYPE REQUIRE- MENTS	RECEIVER TYPE REQUIRED	REMARKS
ES	AT LEAST 3 db ABOVE SIGNAL POWER AT THE TARGET RECEIVER	BW OF THE IR RECEIVER TO BE JAMMED	MANUAL OR AUTO TUNED	HIGH POWER IR SOURCE	IR RECEIVER	
						SPECIAL CASE OF ABOVE SPOT JAMMING (SSB AND DSB) BROADER BAND COVERAGE REQUIRED
ES	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL TUNING	HIGH POWER TUBE, WIDEBAND TUNING OVER NORMAL COMMUNICATIONS BAND OR SELECTED PORTION OF IT	NORMAL AM, FM, OR AM FM	NORMAL TUNABLE TRANSMITTER MAY BE USED IF POWER OUTPUT RF TUNING RANGE ADEQUATE, AND REQUIRED AM OR FM TYPE USED
S	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL OR AUTO TUNED	NOT SPECIAL		THIS TYPE JAMMING WOULD PROBABLY FIND PRIMARY USE AS NUISANCE TO SIGINT ACTIVITIES TO USE UP SEARCH TIME
S	SEVERAL WATTS TO SEVERAL HUNDRED WATTS (AVERAGE)	BW OF TARGET RECEIVER	MANUAL TUNING	NOT SPECIAL	NONE	THIS TYPE JAMMING WOULD PROBABLY FIND PRIMARY USE AS NUISANCE TO SIGINT ACTIVITIES TO USE UP SEARCH TIME.
S	UP TO SEVERAL WATTS	BW OF TARGET RECEIVER	MANUAL OR AUTO TUNED	IR SOURCE OF SEVERAL WATTS CAPABILITY	IR DETECTOR DEMODULATOR	COULD BE USED FOR VOICE CW INSERTION INTO COMMUNICATION NET
S	AT LEAST AS GREAT AS SIGNAL POWER AT TARGET RECEIVER AND PREFERABLY GREATER	BW OF TARGET RECEIVER	MANUAL TUNING	HIGH POWER OVER SELECTER PORTIONS OF BAND	NORMAL AM FM, OR AM FM	MUST KNOW WHICH SIDEBAND ENEMY IS TRANSMITTING ON

FIG 12 -(S) JAMMER REQUIREMENTS FOR COMMUNICATIONS TARGETS (CONT D)

2

SECRET

FREQUENCY	NOMEN- CLATURE	POWER OUTPUT	MODULATION TYPE	MOBILITY	PURPOSE	REMARKS
150-300 kc 190-350 kc	SL-2 SL-2	1 mv 1 mv	AM	UNK	BERLIN TRANSMITTER	
175 kc-12 Mc	FK-500	500 w	AM	MOUNTED IN ZIS-151	COMMUNICATIONS TRANSMITTER	CAN BE USED AS JAMMER
175 kc-12 Mc	FK-50	50 w	AM	TRUCK MOUNTED	COMMUNICATIONS TRANSMITTER	CAN BE USED AS JAMMER
175-kc-12 Mc	FK-3.5	3.5 w	AM	3-MAN PACK	COMMUNICATIONS TRANSMITTER	CAN BE USED AS JAMMER. MARGINAL EFFECTIVENESS DUE TO LOW POWER OUTPUT
250-370 kc	1-A	2 kw		UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
250-750 kc	1-VF	4 kw		UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
250 kc-12 Mc	RAT (AT-1)	1.5 kw	AM	UNK	TACTICAL COMMUNICATIONS TRANSMITTER	CAN BE USED AS JAMMER
300-500 kc	2A; 2D	1 kw		UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
350-700 kc	UNK	20 kw	AM		BROADCAST TRANSMITTER	CAN BE USED AS JAMMER: AT LEAST 50 KNOWN
400-750 kc	3D	25 w		UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
500-1500 kc	HF-2982	100 w	AM: 800 cps, DASHES FM: 20 cps, SWEEP	UNK	COMMUNICATIONS JAMMER	
500-1560 kc	SM-5	5 kw	UNK	MOBILE; TRAILER MTD.	COMMUNICATIONS JAMMER	FIRST BUILT IN 1953; 14 AVAILABLE IN 1955
500-1600 kc	SM-6	2 kw	UNK	FIXED	JAMMER	
500-1700 kc	(BC TRANS- MITTER)	500 kw	AM	UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
520-1050 kc	4A	100 w	UNK	UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER
1.2-11.2 Mc	11 DA	1 kw	UNK	UNK	JAMMER	
2.2-5.7 Mc	11 AK-1	800 w	UNK	FIXED OR MOBILE	JAMMER	
2.5-4.5 Mc	11 AK	800 w	UNK	UNK	JAMMER	
3-30 Mc	(HF-BC TRANSMITTER)	15-120 kw	AM	UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER: OVER 2300 IN USE
3-30 Mc	(VOA-BBC JAMMERS)	2 kw (AVERAGE OF ALL EQUIP- MENTS)	UNK	UNK	VOA-BBC BROADCAST JAMMER	1000 TO 3000 EQUIPMENTS IN USSR AND SATELLITES JAM WESTERN VOA-BBC BROADCASTS
4.1-8.5 Mc	1-VF	4 kw	UNK	UNK	BROADCAST TRANSMITTER	CAN BE USED AS JAMMER

FIG. 13 - (S NOFORN) SOVIET AND SATELLITE COMMUNICATIONS JAMMERS INCLUDING BROADCAST TRANSMITTERS
WHICH CAN BE USED AS JAMMERS

SECRET

Electronic sound deception is effective when visual observation is denied to an adversary because of smoke, fog, cover of darkness, etc. Knowing that his opponent will be utilizing highly sensitive listening devices against him, the enemy can be expected to simulate conditions of battle such as gunfire, troop and vehicle movements, etc., using prerecorded magnetic tapes.

Because of the emphasis in the next decade on subsurface naval vessels, including assault craft carrying personnel and weapons, sonic deception devices will become increasingly important. It will be as advantageous for an enemy to simulate underwater communications traffic (another type of manipulative deception) over low frequency sonic nets as it is on the beach. Since a subsurface attack craft would impose a substantial threat to a convoy comprising the assault force, considerable confusion in the debarkation area could result from a simulated enemy submarine attack. Submarine simulators, capable of being operated as a drone, are already in existence that will simulate hull and screw noises, and provide a sonar return echo. These drones will become more sophisticated in the interim time period, as research into underwater communications results in the capability of the drone's providing subsurface techniques of communication deception. An important function of the submarine simulator would be to decoy the ASW group away from the legitimate undersea threat. The capability of the drone decoy to carry a tape recorder and transmitter, plus a guidance system that would operate via a subsurface TM link, provides the enemy with a substantial confusion factor in the event of a concentrated assault on his position.

A weapon of significant importance that will have to be considered by the planners of a coastline assault is the generation of weather conditions by the enemy. The remesis of most surveillance systems, ground-based or airborne, including the multiple-sensor concept, is a high moisture density ground fog. The water vapor masks the visual, photographic, and TV, from activity beneath, and absorbs the thermal radiation from the ground to an extent that it is undetectable from above. The effect on MTI radar would result in signal attenuation only, but the MTI sensor would be much more vulnerable to the deception techniques already mentioned, because of the absence of back-up data, from the accompanying visual and thermal sensors.

The extent to which this area of technology will be developed by the time period in question is difficult to determine at this time. The current thinking of some meteorologists is that man will never be able to control weather conditions, even

SECRET

SECRET

HRB

on a limited scale, to the degree that it could be used as a tactical weapon. This opinion is based primarily on the tremendous amount of energy that would be necessary to generate clouds, or fog, in an area that does not normally experience that type of weather condition. Because of the instability of wind, moisture, and temperature conditions, therefore, it is theorized that a sustaining man-made cloud or fog cover would be impossible to generate in the Equatorial and Tropical zones of the Earth. In the Moderate and Polar latitudes, however, especially during the night, it is further theorized that man would have the best success in attempting weather modification. Attempts at cloud "seeding," using silver iodide, and more recently, soot particles, have met with some success in producing rain. Because of the dependence upon the inherently consistent weather conditions of a given locality, therefore, the use of weather modification as a tactical weapon seems to be, at present, not feasible.

With technology advancing at its present rate, however, the ability to modify weather by 1980 cannot be completely ruled out, based on current opinion. The capability of being able to do it at all, even on a limited scale, would provide the enemy with the means to move weapons, personnel, and vehicles, at will, much to the frustration of those who must know his location to gain tactical advantage.

SECRET

VII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The study described in this report considered some of the more important factors which must be considered in communications deception for a naval amphibious assault operation in the 1975-1980 time period. Consideration was given to U. S. deception directed against enemy sensors, anti-deception efforts on the part of the enemy, and the threat to U.S. amphibious forces caused by deception efforts on the part of the enemy.

Conventional warfare with the possible limited use of nuclear weapons is assumed. The aspects of all-out nuclear war were not considered.

U.S. amphibious forces must be prepared to meet a wide range of defenses in the 1975-1980 time period. The most sophisticated of these will be the established coastal defenses of the Soviet homeland. Hasty defenses on the flanks of Soviet forces in a theater of operations and the more primitive defenses of less developed nations must also be considered. The degree of deception capability required will vary in accordance with the defenses in the assault area. In general it can be assumed that in most cases the defenses have been established according to Soviet military doctrine or some derivative of it and that the defending forces will employ Soviet material or material of Soviet design. The actual defenses in a specific area will depend to a large degree upon who the enemy is, how long this enemy has occupied the area, and how important the area is considered to be in relation to the overall objectives.

Communications deception as practiced in the amphibious assault area is tactical deception. Strategic deception is practiced in connection with the preparation for assault operations as early as the planning stage. This might take the form of a buildup of dummy traffic on naval communications circuits which can be replaced as necessary by real traffic when the operations reach a stage where additional traffic volume is necessary to prepare for the assault operation. In this manner enemy intelligence cannot determine by analysis of traffic volume that a buildup of real traffic has taken place. Transmission of false information on low security circuits which it is believed enemy intelligence can decipher is also a form of strategic deception which might be useful. It is recognized that these and other forms of strategic deception might be helpful in

connection with an amphibious operation, particularly with early stages. They are not, however, covered in any detail in this report since they do not come under the jurisdiction of the task force commander nor are they performed in the assault areas.

Tactical communications deception in an amphibious assault area in the 1975-1980 time period will be similar to the present day deception. The objectives of the deception will be the same: to confuse the enemy, deny him accurate information, delay his defensive efforts, and increase his reaction time.

Deception operations, specifically those designed to deny information to the enemy and those to further insure our own security, appear to be as important in a future assault operation as does gaining air superiority and isolation of the objective area. It would be foolish to attempt an amphibious assault operation if one could not rely on achieving air superiority and isolation of the objective area. However, the tactical advantage gained by these factors no longer appears to be sufficient to ensure success in future assault operations. Two of the most important factors which influence this condition are: (1) the increased and highly reliable surveillance capability which the enemy of the future will possess and (2) the enemy's ability to rapidly move large units of reserve forces to any threatened coastal area.

Hence, the success of an assault operation must depend, to a certain extent, on successful deception in the areas of denial and security. It would be unwise to plan an assault operation entirely dependent upon deception efforts; however, unless the enemy is uncertain as to which is the main threat aimed against him and the time and location at which it will strike, the chances of a successful assault become rather poor. Moreover, this deception must be successful at least until the assault phase of the operation is underway. Otherwise the enemy will have ample time to move into position to counter the landing.

Therefore, it appears that the future naval amphibious assault operation will embrace a somewhat modified concept concerning deception, inasmuch as it presently requires that success of the amphibious assault depends in no way upon success of the deception operations. The contention is that some reliance on deception will be necessary in the formulation of an amphibious assault plan.

It became apparent during the course of the study that one of the most critical elements contributing to the success or failure of an assault operation was the factor of time. Moreover, this element will play a more prominent role in the future than it has in the past. Based upon the Soviet strategy of coastline defenses, in which the front line fortifications are lightly manned and highly mobile reserve units are prepared to reinforce any threatened area on very short notice, it becomes evident that the assaulting forces must establish a tenable beachhead prior to the arrival of enemy reserves if the assault is to be successful. It does not appear feasible, therefore, that a successful landing could be made on the beaches of an enemy shoreline if all available enemy reserve forces were deployed to defend those beaches, and it is precisely with these conditions that the planners of all future assault operations will be faced. The essential requirement, then, is to use deception as one method of gaining time to get our first forces ashore before enemy reinforcements can be deployed. The deception to be used before a landing has two distinct related requirements. Manipulative deception must be carefully planned and executed and coordinated with noncommunications deception efforts in order to deceive the multisensor, rapid-display type of intelligence likely to be used by the defending forces. Closely related to this is the control of the regular communications facilities of the task force. The role of the regular facilities will range from complete silence to that of participation through the transmission of deceiving information.

Imitative deception (intrusion into an enemy communication system to introduce false or misleading information) is best used after the assault forces reach the beach. It is almost always directed against low echelon nets, where their mobility and rapidly changing requirements usually dictate plain text voice transmission. Higher echelon nets will be less susceptible to imitative deception due to the type of system used (wire, optical, etc.); type of transmission (burst, pseudo-noise, teletype, etc.); authentication procedures; and the security of the messages (crypto).

Jamming has been considered in this study as a deception technique. It can be used in conjunction with other deception or as a last resort when all other deception fails. When continuous jamming is used there is little doubt on the part of the enemy as to its intent, and its source can be located by radio direction finding techniques.

Naval transportation vehicles of the 1975-1980 time period, although not a subject of this study, have been considered in connection with the communications deception requirements to ensure compatibility. Little change in the types of ships is foreseen. Ships will be faster, better armed, and more versatile. Submarine troop carriers and transports might be possible even though current thinking discounts this due to the extremely high cost/weight/volume ratio. Even if future developments produce vehicles drastically different from those of today, communications deception can prove assistance during the time required for U.S. forces to establish a firm beachhead. Movement of troops and equipment from the transport ships to the area of enemy contact may be by boat, hydrofoil, ground effects machines, helicopters, VTOL aircraft, or other vehicle. The method of transport changes little in the communications deception requirements except timing.

B. RECOMMENDATIONS FOR RESEARCH AND DEVELOPMENT

In the following subsections specific recommendations concerning further investigation, research, and development in the two types of communications deception are outlined.

1. Manipulative Deception

For the development of U.S. naval communications deception techniques to provide the enemy with false or misleading information concerning U.S. amphibious assault operations, the following specific investigations should be pursued:

(1) Continued research to deceive multisensor equipments by use of decoys or small ships bearing deception equipment. The predictable advances in photography, both in the IR and visual ranges, will result in the requirement of very realistic deception efforts. Not only must dispersion of decoys be realistic, but IR radiations must resemble those of the simulated vessel. It may be possible by high resolution photography to determine shape of vessels. This would present a serious problem to the use of decoys. (Ref. pgs. 76, 77, 78, 79, 81, 83, 84, 85).

(2) Development of techniques to vary characteristics of U.S. deceptive equipments so they are not easily identified. In manipulative deception, dummy nets are established which give the appearance of many stations when in reality they come from one transmitter controlled by a tape recorder and a voice controlled relay. In this type of operation a fixed relationship exists between

the time the RF carrier is turned on and the beginning of the voice. There is a similar fixed delay after the voice stops before the carrier goes off. These times are usually very short and the average intercept operator is not aware of them. It is within our capability today to develop a set of equipments which would display these time relationships. In a normal operation these will appear as random times, but in a manipulative deception situation, as we know it today, the pattern is not random but fixed. Similarly each transmission can be examined for frequency deviation from the previous transmission. By adjusting the sensitivity to frequency change it should be possible to identify separate transmitters and even alert an intercept operator by a bell or flashing light if the signals appear to be coming from the same transmitter. Time and frequency are only two of the variables which might be used to detect manipulative deception. There are others.

The parameters of the deception transmitter could be varied by the use of special circuitry between the tape recorder and transmitter to provide the necessary changes in time, frequency, and other variables. This might require one additional tape recorder channel for each transmitter. It would require modification of the transmitter or building of a new transmitter along with the construction of control circuitry. (Ref. pgs. 54, 55, 56)

(3) Investigation of possible neutralization and/or destruction of enemy surveillance platforms, either airborne or satellite. It appears that the most economical method of neutralizing a surveillance system is not the nullification of the capability of the platform's sensors, but destruction of the platform itself. Since the artificial satellite will play a significant role as the reconnaissance platform of the future, a weapons system must be developed that would be capable of identifying and destroying an enemy's military satellites in a future "hot war." This should be of particular interest to the Navy since the presence of enemy aerospace surveillance platforms will hinder the successful strategic movement of ships at sea that heretofore depended upon the vastness of the oceans for cover. It might be more advantageous at times, however, to neutralize the surveillance sensors and permit the platform to function as before, since this would not necessarily compromise a neutralization capability. Hence, neutralization of sensors as well as destruction of platforms requires considerable investigation. (Ref. pgs. 13, 24, 25, 26, 27, 79, 80, 81, 83)

(4) Investigation of techniques of the enemy's communication intelligence gathering efforts with special emphasis on the time required to collect, correlate, evaluate, and disseminate intelligence information. Since our manipulative deception efforts will be aimed at the enemy's communications intelligence system, a detailed knowledge of how this system operates is a prerequisite to deception planning. (Ref. pgs. 11, 12, 31, 32, 33, 36, 37, 81)

(5) Further investigation of the generation and transmission of false information over our own active communication circuits. (Ref. pgs. 53, 54, 55, 76)

(6) Investigation of techniques to efficiently control dummy traffic nets which are used specifically in deception activities. (Ref. pgs. 11, 12, 53, 54, 55)

(7) Acoustic deception methods for covering the acoustic communications of submarines and other naval vessels. Underwater acoustic communications can be used for submarine to submarine, from submarine to ship, and from ship to ship. The range is short relative to radio communications; however, it compares favorably with IR, visual and microwave communications. In an amphibious operation, especially if conducted under cover of heavy weather or fog, acoustic communications can provide adequate range and are not hampered by atmospheric conditions.

The following areas merit close investigation:

Development of underwater communications for use in amphibious operations (Ref. pg. 40, 41)

Development of underwater noise sources to mask communications. The same sources might be helpful in masking ship noises of the actual assault forces (Ref. pgs. 54, 100)

Integration of underwater deception sounds with radio, visual, electromagnetic, and other deception efforts to deceive complex multisensor systems. (Ref. pgs. 54, 100)

(8) Continued improvement in the speed at which naval assault craft can approach the beach. The concept of beaching LSTs and other large assault craft prior to disembarkation of troops and equipment offers many

advantages to the assaulting forces. The speed with which the assault is carried out is critical when one considers the enemy's capability to move his reserve forces. Thus the more rapid the beach approach, the quicker a tenable beachhead can be established. (Ref. page 16)

(9) Generation of weather conditions to include, as a minimum, fog or haze conditions of one to four hours duration. The ability to generate clouds or fog, even on a small scale as compared to natural conditions, would provide ships at sea as well as forces on land with a substantial deterrent against the effectiveness of multisensor surveillance. Although, in the past, smoke has been used on land and sea as a screen against visual observation, the sophistication of present and future thermal and radar sensors makes obsolete this technique of camouflage. The infrared and high resolution radar systems contained in the integrated surveillance platform of the future are susceptible only to a water vapor suspension in air as a means of negating their value in a tactical situation.

A method, therefore, of generating fog or cloud cover, over perhaps only one square mile, would provide a solution to the problem of concealing identity, in the case of ships at sea, or movement of men and vehicles on land, from the enemy's observation platforms. Research into weather modification, for this purpose, should be given serious consideration by the Navy where geographical conditions make this technique feasible. (Ref. pgs. 13, 58, 81, 100, 101)

4. Imitative Deception

For the development of U. S. naval communications deception techniques to intrude into enemy communications nets, the following specific investigations should be pursued:

(1) Development of linguistic capability within the existing deception units as well as increasing the number of such units to meet the deception requirements of the future. Unless sufficient deception specialists are available to all the activities associated with an assault operation the enemy is given the opportunity to determine, with greater certainty, our intentions. Moreover, without a linguistic capability the tactical deception units will be unable to exploit many of the advantages of imitative deception. (Ref. pg. 63, 64)

(2) Investigation of methods of intrusion into the wire communications nets of the enemy both from the standpoint of intelligence gathering and imitative deception efforts. Estimates concerning enemy communications indicate that primary emphasis will be placed on wire communications for use in defensive situations. If imitative deception is to be successful, techniques must be developed for intruding into the enemy's wire nets. (Ref. pg. 57)

(3) Development of equipments with operating characteristics similar to those of the enemy. In order to be successful in imitative deception efforts, the deception units must be able to imitate equipments as well as the communications they transmit. The capture of enemy equipments provides one solution to this problem. (Ref. pg. 58)

(4) Development of stable lock and track devices for use in optical communications systems. Many advantages are offered by communications of this nature; however, due to narrow bandwidth, the present difficulty of establishing and then maintaining contact limits their use. (Ref. pgs. 14, 47, 79)

(5) Investigation of the psychological framework within which the enemy is operating and prescribing those actions and events which will make him most susceptible to deception. Not until the Korean conflict did anyone realize the potential of psychological techniques in warfare. The indoctrination of American POWs by communist officials produced some rather surprising results. Hence it appears that psychological techniques, if properly applied, do influence human beings to act in predictable ways. Therefore, considerable effort should be exerted in the investigation of these psychological aspects and their application in influencing the behavior of enemy soldiers.

SECRET

HRB

APPENDIX: SUPPLEMENTARY INFORMATION

-111-

SECRET

SECRET

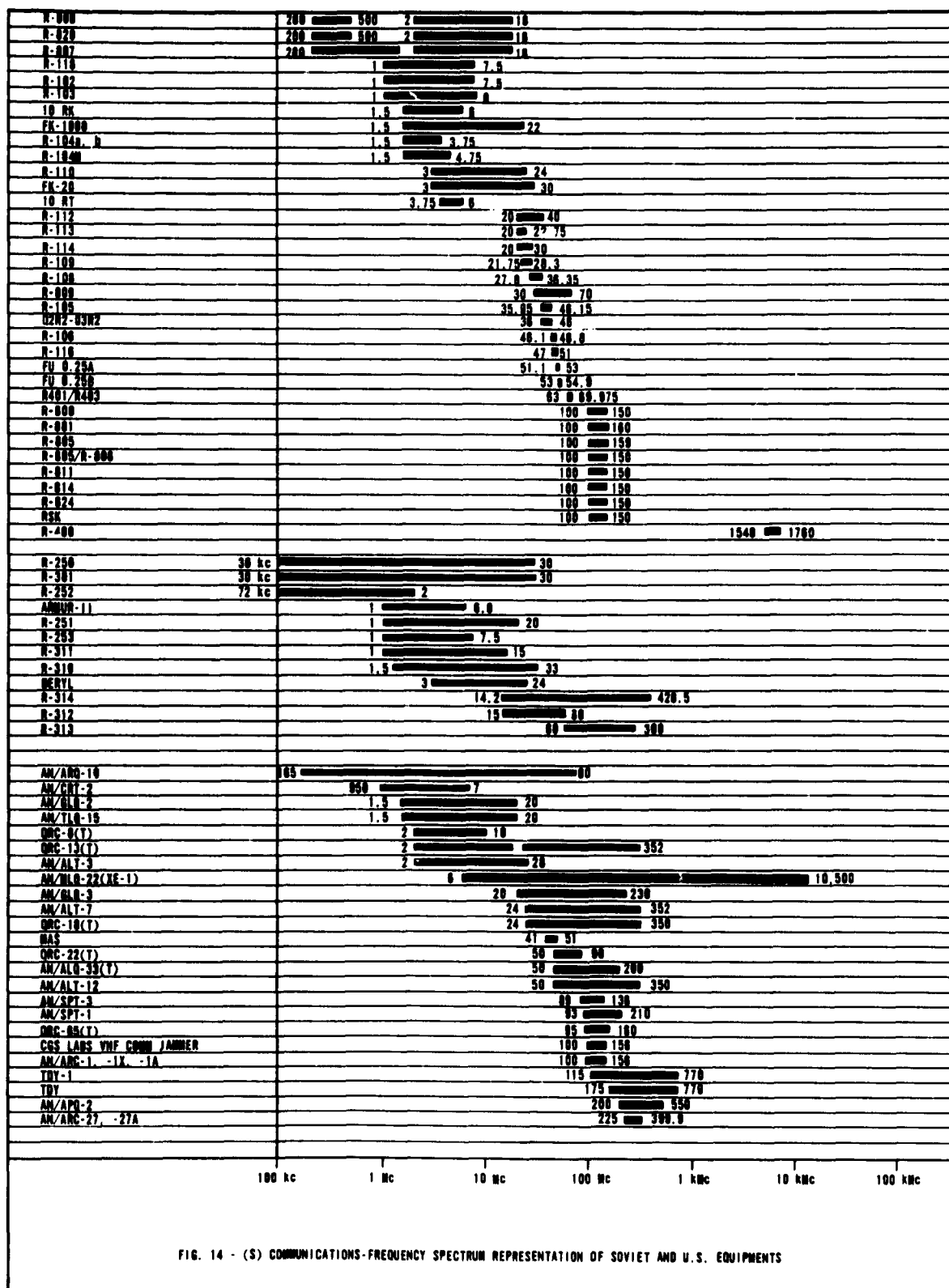


FIG. 14 - (S) COMMUNICATIONS-FREQUENCY SPECTRUM REPRESENTATION OF SOVIET AND U.S. EQUIPMENTS

SECRET

SECRET

FIG 15 (S) SOVIET COMMUNICATIONS EQUIPMENT

DESIGNATION	FREQUENCY RANGE (Mc)	MODULATION	POWER OUTPUT	NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF RECEPTION	RECEIVER SENSITIVITY	RECEIVE BANDWIDTH
D2R2 D1R1	0 0 46 1	UNKNOWN	UNKNOWN	201 WITHIN FREQUENCY RANGE EACH SET OPERATES ON ONLY ONE CHANNEL WITHIN BAND	POSSIBLY SUPER REGNERATIVE	VOICE	5 MICROVOLTS FOR S/N RATIO OF 15DB	UNKNOWN
10RK	1 5 6 0	AM	NOT MORE THAN 10 WATT	PROBABLY BOTH FREE TUNING AND 1 OR 2 CRYSTAL CONTROLLED PRE SET FREQUENCIES	SUPERHET	VOICE MORSE	UNKNOWN	UNKNOWN
10RT	3 75 6 0	AM	5 6 WATTS	FREE TUNING OP 1 OR 2 CRYSTAL CONTROLLED PRESET FREQUENCIES	SUPERHET	VOICE MORSE	UNKNOWN	UNKNOWN
FK20	HF	SSB	UNKNOWN	UNKNOWN	PROBABLY SUPERHET	VOICE PROBABLY ALSO AM VOICE	UNKNOWN	UNKNOWN
FK1000	1 5 22 0	AM FSK	300 W (VOICE) 1000 W (CW)	MINIMUM INTERVAL BETWEEN CHANNELS SAID TO BE 50 kc (411 CHANNELS WITHIN TUNING RANGE INDICATED)	PROBABLY SUPERHET	VOICE MORSE RTT VOICE RTT ¹	UNKNOWN	REPORTEDLY TABLE FOR 750 OR 3000
FJ0 15	1 53 0 54 9 0 51 1 53 0	FM	0 25 WATT	20 WITHIN FREQUENCY RANGES OF A AND 9 AT 100 kc INTERVALS	SUPERHET	VOICE	1 2 UV 60 OHM IN- PUT WITH BAND- WIDTH OF 50 kc MEASURED THROUGH- OUT AND 20DB S/N RATIO	UNKNOWN
R 102	1 7 5 (NOMINAL)	AM FSK	300 W (VOICE) 1000 W (MORSE) 1000 W (RADIO PRINTER)	UNKNOWN PROBABLY SAME AS R 103	USES AMUR 11 AND R-253 OR R 311	AMUR 11 VOICE MORSE RTT VOICE RTT R-253 OR R-311 VOICE MORSE	AMUR 11 UNKNOWN R 253 UNKNOWN R 311 6-8 UV VOICE 3 UV MORSE ²	AMUR 11 N APPROX 1-1 R 253 UNK R 311 MIN APPROX 0 5
R 103	TRANSMITTER 1 0 8 0 Mc AMUR 11 REV ¹ 1 0- 8 0 Mc R-311 PCVR 1 0- 15 0 Mc	MORSE VOICE FSK VOICE FSK ¹ MORSE VOICE FSK VOICE FSK VOICE MORSE	120 WATTS NOMINAL	CHANNELS AT 1 kc INTERVALS BETWEEN 1 & 2 kc INTERVALS BETWEEN 2 & 4 Mc AND AT 4 kc INTERVALS BETWEEN 4 & 8 Mc AMUR 11 HAS SIMILAR CHARACTER ISTICS	AMUR 11 SUPERHET R 311 SUPERHET	AMUR 11 VOICE MORSE RTT VOICE RTT R 311 VOICE MORSE	AMUR 11 UNKNOWN R 311 6-8 UV VOICE 3 UV MORSE ²	AMUR 11 M1 APPROX 1-1 R 311 MIN APPROX 0 5
R 104	R 104 a & b 1 5 3 75 TWO BANDS R 104M 1 5 4 75 TWO BANDS	AM	a 5W (VOICE) 10W (MORSE) b 1-3W (VOICE) 3-5W (VOICE) W (VEHICULAR) 10W (VOICE) 20W (MORSE) W (MAN-PACK) 5W (VOICE) 10W	TRANSMITTER HAS A FIXED NUMBER OF FREQUENCIES AT 10 kc INTERVALS. RECEIVER IS CONTINUOUS TUNING	PROBABLY SUPERHET	VOICE MORSE	UNKNOWN	UNKNOWN
R 105	35 94 46 15	FM	1 3 W	205 AT 05 Mc INTERVALS	SUPERHET	FM VOICE	1 5 MICROVOLTS	UNKNOWN
R 106	46 1 48 8	AM	0 5-0 8 WATTS	18 CHANNELS	PROBABLY SUPER HET	VOICE	UNKNOWN	UNKNOWN
R 108	27 8 36 35	FM	REPORTEDLY 1 2 W	172 AT 05 Mc INTERVALS	SUPERHET	FM VOICE	1 5 MICROVOLTS ¹	UNKNOWN
R 109	21 15 28 3	FM	REPORTEDLY 1 2 W	144 AT 05 Mc INTERVALS	SUPERHET ¹	FM VOICE	1 5 MICROVOLTS ¹	UNKNOWN
R 110	3 0 24 0	AM FSK	REPORTEDLY 15 kw (PROBABLY MORSE AND RADIO PRINTER ONLY LESS FOR VOICE)	UNKNOWN POSSIBLY BASED ON PRINCIPLES USED IN R 103	BERYL PROBABLY SUPER- HET R 250 PROBABLY SUPERHET	BERYL VOICE MORSE PTT VOICE RTT R 250 VOICE MORSE	UNKNOWN	UNKNOWN

1

SECRET

SECRET

FIG 15 (S) SOVIET COMMUNICATIONS EQUIPMENT

NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF RECEPTION	RECEIVER SENSITIVITY	RECEIVER BANDWIDTH	RECEIVER SELECTIVITY	ANTENNA	INSTALLATION	REMARKS
FREQUENCY RANGE OPERATES ON ONLY ONE MIN BAND	POSSIBLY SUPERHET	VOICE	5 MICROVOLTS FOR S/N RATIO OF 150B	UNKNOWN	UNKNOWN	PRESUMABLY KULIKOV WHIP	MAN-PACK	SET LOOKS LIKE AN IMPROVED VERSION OF THE R 116
WITH FREE TUNING AND TAL CONTROLLED PRE CIES	SUPERHET	VOICE MORSE	UNKNOWN	UNKNOWN	UNKNOWN	WHIP	USED IN COMMAND VEHICLES AND SOME ASSAULT GUN VEHICLES	
OR 1 OR 2 CRYSTAL PRESET FREQUENCIES	SUPERHET	VOICE MORSE	UNKNOWN	UNKNOWN	UNKNOWN	WHIP	USED IN APC'S AND SOME TRUCKS	
	PROBABLY SUPERHET	VOICE PROBABLY ALSO AM VOICE	UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN	MAN-PACK	
ERVAL BETWEEN 10 TO BE 50 kc LS WITHIN TUNING ATED)	PROBABLY SUPERHET	VOICE MORSE RTT VOICE RTT ¹	UNKNOWN	REPORTEDLY ADJUST- TABLE FOR 300 750 OR 3000 cps	UNKNOWN	UNKNOWN	DESIGNED TO BE INSTALLED IN SINGLE VEHICLE	1 VOICE RTT SIMULTANEOUS VOICE AND FSK
FREQUENCY RANGES OF 100 kc INTERVALS	SUPERHET	VOICE	1.2 UV 60 OHM IN- PUT WITH BAND- WIDTH OF 50 kc MEASURED THROUGH- OUT AND 200B S/N RATIO	UNKNOWN	IMAGE FREQ RE- JECTION MIN 400B ADJACENT CHANNEL REJECTION MIN 600B	QUARTER WAVE STEEL TAPE OR LONG WIRE	MAN-PACK	RECEIVER CIRCUIT INCLUDES SQUELCH WITH ON-OFF SWITCH
BABLY SAME AS R 103	USES AMUR 11 AND R 253 OR R 311	AMUR 11 VOICE MORSE RTT VOICE RTT R 253 OR R 311 VOICE MORSE	AMUR 11 UNKNOWN R 253 UNKNOWN R 311 6-8 UV VOICE 3 UV MORSE ¹	AMUR 11 MINIMUM APPROX 1-1.5 kc ² R 253 UNKNOWN R 311 MINIMUM APPROX 0.5-1.0 kc ²	AMUR 11 UNKNOWN R 253 UNKNOWN R 311 UNKNOWN USED XTAL FILTER WITH PHASING CONTROL	WHIP DIPOLE MAST	INSTALLED IN TWO ZIS 151 VEHICLES	1. REPORTED, NOT ON BASIS OF EQUIPMENT EXAMINATION 2. TENTATIVE, BASED ON EXAMINATION OF CIRCUIT DIAGRAMS.
1 kc INTERVALS 2 kc INTERVALS 4 kc AND AT 4 kc BETWEEN 4 & 8 Mc SIMILAR CHARACTER	AMUR 11 SUPERHET R 311 SUPERHET	AMUR 11 VOICE MORSE RTT VOICE RTT R 311 VOICE MORSE	AMUR 11 UNKNOWN R 311 6-8 UV VOICE 3 UV MORSE ²	AMUR 11 MINIMUM APPROX 1-1.5 kc ³ R 311 MINIMUM APPROX 0.5-1.0 kc ³	AMUR 11 UNKNOWN R 311 UNKNOWN USES XTAL FILTER WITH PHASING CONTROL. HAS NO ELECTRICAL BAND- SPREAD	TRANSMITTER DOUB- LET MAST BEVER- AGE RECEIVER DOUBLET WHIP LONG WIRE	MOUNTED IN SHELTER ON ZIL-157 VAN	EXAMINED R-103 CAPABLE OF SIMPLE OPER- ATION ONLY 1 VOICE FSK-SIMULTANEOUS VOICE AND FREQUENCY SHIFT KEYING 2. REPORTED, NOT ON BASIS OF EXAMINA- TION 3. TENTATIVE, BASED ON EXAMINATION OF CIRCUIT DIAGRAMS
HAS A FIXED FREQUENCIES AT 10 kc RECEIVER IS TUNING	PROBABLY SUPERHET	VOICE, MORSE	UNKNOWN	UNKNOWN	UNKNOWN	WHIP, WIRE DIPOLE, TELESCOPIC MAST TUNING CIRCUITRY AND CONTROL INCORPORATED	R-104a - USED IN GAZ-69 R-104b - MAN-PACK R-104m - BOTH GAZ-69 AND MAN-PACK	
Mc INTERVALS	SUPERHET	FM VOICE	1.5 MICROVOLTS	UNKNOWN	-20B AT 25 kc 1000B AT 60 kc	KULIKOV WHIP 40- METER LONG WIRE TUNING CIRCUITRY AND CONTROL INCOR- PORATED	MAN-PACK ALSO MOUNTED IN GAZ-69 WITH R-104	TRANSMITTER FREQUENCY DEVIATION NOW INALLY 7 kc. DRIFT LESS THAN 8 kc AFTER 5 MINUTE WARM-UP. RECEIVER HAS AFC WITH ON-OFF SWITCH. AFC HOLDS 150 UV SIGNAL OVER +50 kc RANGE. INFO MATION APPLIES TO LATEST KNOWN MODEL R-105D
S	PROBABLY SUPER- HET	VOICE	UNKNOWN	UNKNOWN	UNKNOWN	KULIKOV WHIP 30- METER LONG WIRE TUNING CIRCUITRY AND CONTROL IMPLIED	MAN-PACK	
Mc INTERVALS	SUPERHET	FM VOICE	1.5 MICROVOLTS ¹	UNKNOWN	-20B AT 25 kc 1000B AT 60 kc ¹	KULIKOV WHIP DOUB- LET LONG WIRE TUNING CIRCUITRY AND CONTROL IMPLIED	MAN-PACK	1 INDICATED BY R-105D TO WHICH R-108 IS SIMILAR EXCEPT FOR FRE- QUENCY RANGE. LATEST MODEL IS R-108D. REMARKS UNDER R 105 PROBABLY ALSO APPLY
Mc INTERVALS	SUPERHET ¹	FM VOICE	1.5 MICROVOLTS ¹	UNKNOWN	-20B AT 25 kc 1000B AT 60 kc ¹	KULIKOV WHIP DOUB- LET LONG WIRE	MAN-PACK	1 INDICATED BY R-105D TO WHICH R-109D, REMARKS UNDER R 105 PROBABLY ALSO APPLY
POSSIBLY BASED ON USED IN R 103	BERYL PROBABLY SUPER- HET R 250 PROBABLY SUPERHET	BERYL VOICE MORSE PTT VOICE RTT R 250 VOICE MORSE	UNKNOWN	UNKNOWN	UNKNOWN	UNK V OR RHOMBIC PROBABLE	INSTALLED IN 5 COMMUNICATING VEHICLES	

SECRET

2

SECRET

FIG 15 - (S) SOVIET COMMUNICATIONS EQUIPMENT (CONT D)

DESIGNATION	FREQUENCY RANGE (Mc)	MODULATION	POWER OUTPUT	NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF PERCEPTION	RECEIVER SENSITIVITY	RECEIVING BANDWIDTH
R-112	20-40 Mc PORTION OF FREQUENCY SPECTRUM	BELIEVED TO BE AM	PROBABLY NOT MORE THAN 20 WATTS	REPORTEDLY 220 CHANNELS. INTERVAL BETWEEN CHANNELS IS POSSIBLY 25 kc	PROBABLY SUPERHET	VOICE POSSIBLY ALSO MORSE	UNKNOWN	UNKNOWN
R-113	20-22 375	BELIEVED TO BE AM	PROBABLY 8-10 WATTS	96 AT 25 kc INTERVALS. PROBABLY AT LEAST 4 CHANNELS CAN BE PRESET	PROBABLY SUPERHET	VOICE POSSIBLY ALSO MORSE	UNKNOWN	UNKNOWN
R-114	20-30 Mc PORTION OF FREQUENCY SPECTRUM	AM IMPLIED BY USAGE	BETWEEN 1 AND 2 WATTS	UNKNOWN	PROBABLY SUPERHET	VOICE	UNKNOWN	UNKNOWN
R-115	APPROXIMATELY 47-51 Mc	AM	0.1-0.5 WATTS	10 CHANNELS	SUPER-REGENERATIVE	VOICE	UNKNOWN	MINIMUM APPROX 2 kc ¹
P-118	1.0-7.5	AM FM	50-100 WATTS	FIXED NUMBER OF FREQUENCIES WITH CRYSTAL AND MASTER OSCILLATOR. POSSIBLY SAME AS R-103	AMUR-11 R-311	AMUR-11 VOICE MORSE RTT VOICE RTT R-311 VOICE MORSE	AMUR-11 UNKNOWN. R-311 6-8 UV VOICE. 3 UV MORSE ¹	AMUR-11 MINIMUM APPROX 1.5 kc ² R-311 MINIMUM APPROX 0.5-1.0 kc ²
R-400	1540-1760	PULSE POSITION MODULATION	6-10 WATTS 8.0 WATTS PEAK REPORTED	AT LEAST SIX DUPLEX SPEECH CHANNELS	UNKNOWN	VOICE. PROBABLY MORSE AND RADIO-PRINTER	UNKNOWN	UNKNOWN
P-401 R-473	R-401 LC 0.1-9.945 R-401M BELOW 66.0	FM	1-5 WATTS	54 FOR R-401 WITH 75 kc SPACING. NUMBER OF SIMULTANEOUS CHANNELS 4(2 VOICE, 2 RADIO-PRINTER EACH VOICE CHANNEL CAN BE FURTHER MULTIPLEXED TO PROVIDE 3 RADIO-PRINTER CHANNELS)	PROBABLY SUPERHET	VOICE INVERTED VOICE. RADIO-PRINTER. USE OF FACSIMILE ALSO POSSIBLE	UNKNOWN	UNKNOWN
AMUR-11	1.0-8.0	SUPERHET	AM FSK		VOICE MORSE RTT. VOICE RTT ¹	UNKNOWN	MINIMUM APPROX 1-1.5 kc ²	UNKNOWN
RFYL	PROBABLY 3.0-24.0	SUPERHET	AM FSK		VOICE MORSE RTT. VOICE RTT	UNKNOWN	UNKNOWN	UNKNOWN
R-250	PROBABLY 30 kc 30.0 Mc	PROBABLY SUPERHET	AM		VOICE MORSE AUTOMATIC MORSE WITH ANCILLARY DEVICE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-251	1.0-20.0	PROBABLY SUPERHET	AM		VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-252	72 kc 7.0 Mc	PROBABLY SUPERHET	AM		VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-253	1.0-7.5 (NOMINAL)	PROBABLY SUPERHET	AM		VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-254	PROBABLY 30 kc 30.0 Mc	PROBABLY SUPERHET	AM		VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-300	VHF	PROBABLY SUPERHET	PROBABLY AM & FM		UNKNOWN	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-310	1.0-33.0	PROBABLY SUPERHET	AM		VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-311	1.0-15.0	SUPERHET	A.		VOICE MORSE	0-3 UV VOICE 3 UV MORSE	MINIMUM APPROX 0.5-1.0 kc ²	UNKNOWN. USE CRYSTAL FILTER WITH PHASING TROL HAS NO ELECTRICAL BANDSP
R-312	1.0-60.0	PROBABLY SUPERHET	PROBABLY AM & FM		PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-313	1.0	PROBABLY SUPERHET	PROBABLY AM & FM		PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R-314	1.0-40.0	PROBABLY SUPERHET	PROBABLY AM & FM		UNKNOWN	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN

1

SECRET

SECRET

FIG 15 - (S) SOVIET COMMUNICATIONS EQUIPMENT (CONT D)

NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF RECEPTION	RECEIVER SENSITIVITY	RECEIVER BANDWIDTH	RECEIVER SELECTIVITY	ANTENNA	INSTALLATION	REMARKS
ONLY 220 CHANNELS. IN-BETWEEN CHANNELS IS 25 kc	PROBABLY SUPERHET	VOICE POSSIBLY ALSO MORSE	UNKNOWN	UNKNOWN	UNKNOWN	WHIP	USED IN TANKS APC'S AND OTHER COMMAND VEHICLES	
1 kc INTERVALS. PROBABLY AT LEAST 4 CHANNELS CAN BE USED	PROBABLY SUPERHET	VOICE POSSIBLY ALSO MORSE	UNKNOWN	UNKNOWN	UNKNOWN	WHIP	USED IN TANKS APC'S & SOME TRUCKS	
	PROBABLY SUPERHET	VOICE	UNKNOWN	UNKNOWN	UNKNOWN	PROBABLY KULIKOV WHIP. DOUBLET. LONG WIRE	MAN-PACK	
ELS	SUPER-REGENERATIVE	VOICE	UNKNOWN	MINIMUM APPROX 2 kc ¹	RELATIVELY POOR ¹	KULIKOV WHIP	MAN-PACK	1 BASED ON EXAMINATION OF CIRCUIT DIAGRAM
NUMBER OF FREQUENCIES STAL AND MASTER OR, POSSIBLY SAME AS	AMUR-11 R-311	AMUR 11 VOICE MORSE RTT. VOICE RTT R-311 VOICE MORSE	AMUR 11 UNKNOWN R-311 6-8 UV VOICE. 3 UV MORSE ¹	AMUR 11 MINIMUM APPROX 1-1.5 kc ² R-311 MINIMUM APPROX 0.5-1.0 kc ²	AMUR 11 UNKNOWN. R-311 UNKNOWN. USE CRYSTAL FILTER WITH PHASING CONTROL. HAS NO ELECTRICAL BAND-SPREAD	WHIP. DIPOLE. TELESCOPIC MAST	R-118a. ONE OF THE ZIL SERIES TRUCKS R-118b. ARMORED PERSONNEL CARRIER	1 REPORTED NOT ON BASIS OF EQUIPMENT EXAMINATION 2 TENTATIVE. BASED ON EXAMINATION OF CIRCUIT DIAGRAMS
SIX DUPLEX SPEECH	UNKNOWN	VOICE. PROBABLY MORSE AND RADIO-PRINTER	UNKNOWN	UNKNOWN	UNKNOWN	TWO 5-6 1/2 FEET PARABOLIC DISHES	STATION INSTALLED IN AT LEAST TWO VEHICLES	
401 WITH 75 kc NUMBER OF SIMULTANEOUS CHANNELS. 412 VOICE. 2 AFTER EACH VOICE CAN BE FURTHER MULTI-3 PROVIDE 3 RADIO-CHANNELS	PROBABLY SUPERHET	VOICE. INVERTED VOICE. RADIO-PRINTER. USE OF FACSIMILE ALSO POSSIBLE	UNKNOWN	UNKNOWN	UNKNOWN ¹	ARRAY OF 4 VERTICAL YAGIS AND 4 HORIZ	INSTALLED IN GAZ-63 TRUCK	1 INDICATION OF RECEIVER REJECTION GIVEN BY PRACTICE OF SEPARATING TRANSMISSION AND REJECTION FREQUENCIES BY 27 CHANNELS (e.g. TRANSIT ON CHANNEL 1. RECEIVE ON CHANNEL 28) TO REDUCE CROSS STALK
	VOICE. MORSE RTT. VOICE RTT ¹	UNKNOWN	MINIMUM APPROX 1-1.5 kc ²	UNKNOWN	DOUBLET. WHIP. LONG WIRE. USES SALON COILS FOR IMPEDANCE MATCH	INSTALLED IN SOVIET R-102. R-103 AND R-118 STATIONS		1 VOICE RTT - SIMULTANEOUS VOICE AND RADIO-TELETYPE 2 TENTATIVE. BASED ON EXAMINATION OF CIRCUIT DIAGRAMS PROBABLY ALSO HAS R-154 DESIGNATION
	VOICE. MORSE RTT. VOICE RTT	UNKNOWN	UNKNOWN	UNKNOWN	PROBABLY LONG WIRE DIPOLE. WHIP	INSTALLED IN SOVIET R-110 STATIONS		
	VOICE. MORSE AUTOMATIC MORSE WITH ANCILLARY DEVICE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	PROBABLY LONG WIRE DIPOLE. WHIP	INSTALLED IN SOVIET R-110 STATIONS OR FIXED		REPORTEDLY ALSO IN USE FOR COMINT
	VOICE. MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	KULIKOV WHIP. LONG WIRE	CAN BE MOUNTED IN VEHICLE		USED IN COMMUNICATIONS AND WARNING NETS.
	VOICE. MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	PROBABLY LONG WIRE	UNKNOWN		REPORTEDLY IN USE FOR COMINT
	VOICE. MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	4 METER WHIP	INSTALLED IN SOME R-102 STATIONS		
	VOICE. MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	UNKNOWN	REPORTEDLY VAN MOUNTED		REPORTED IN USE FOR DF. POSSIBLY ALSO USED FOR MONITORING ENEMY NETS AND IN FRIENDLY COMMUNICATIONS NETS
	UNKNOWN	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN VEHICLE OR FIXED		CONFUSING DATA EXISTS. R-304 ALSO REPORTED AS RADIO RELAY AND AS R-330
	VOICE. MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN VEHICLE OR FIXED		USED EITHER WITH UNKNOWN TRANSMITTER FOR COMMUNICATIONS OR FOR COMINT
	VOICE. MORSE	6-8 UV VOICE 3 UV MORSE	MINIMUM APPROX 0.5-1.0 kc ²	UNKNOWN. USES CRYSTAL FILTER WITH PHASING CONTROL. HAS NO ELECTRICAL BANDSPREAD	WHIP. DOUBLET. LONG WIRE	USED IN R-102 R-103 AND R-118 STATIONS		1 REPORTED NOT ON BASIS OF EQUIPMENT EXAMINATION 2 TENTATIVE. BASED ON EXAMINATION OF CIRCUIT DIAGRAMS
	PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	SAME AS OR HIGHLY SIMILAR TO CHUCK LUCK	UNKNOWN		PROBABLY USED FOR BOTH COMMUNICATIONS AND COMINT
	PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	PROBABLY CHUCK LUCK TYPE	UNKNOWN		REPORTED IN USE FOR AIR GROUND COMMUNICATIONS. COMINT USE ALSO PROBABLY
	UNKNOWN	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	UNKNOWN	UNKNOWN		USE UNKNOWN. POSSIBLY USED FOR COMINT

SECRET

SECRET

FIG 15 - (S) SOVIET COMMUNICATIONS, EQUIPMENT (CONT D)

DESIG NATION	FREQUENCY RANGE (Mc)	MODULATION	POWER OUTPUT	NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF RECEPTION	RECEIVER SENSITIVITY	RECEIVER BANDWIDTH
R 318	PROBABLY LF, MF, HF	PROBABLY SUPER- HET	PROBABLY AM		PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN
R 330	R 330 MAY EXIST SINGLE SOURCE OF INFORMATION GIVEN THIS DESIGNATION AS ALTERNATIVE TO R 305							
R 800	100 150	AM	6 WATTS (AIRBORNE USE ONLY)	601 AT 83.3 kc INTERVALS	SUPERHET	VOICE PULSE (WITH ADDITIONAL EQUIP- MENT)	5 10 UV	100 kc (1F)
R 801	100 150 POSSIBLY TO 160	AM	10 WATTS	SIX PRESET CHANNELS. PREVIOUSLY REPORTED 601 CHANNELS AT 83.33 kc INTERVALS BUT MAY HAVE ONLY 240 CH AT 250 kc INTERVALS	SUPERHET	VOICE PULSE (WITH ADDITIONAL EQUIP)	5 UV	100 kc (1F)
R 802	100 159.9	AM	18 20 WATTS	WITHIN THE TUNING RANGE. 514 CH AT 100 kc INTERVALS 19 CH PRESET TO SPECIFIC FRE- QUENCIES WHILE 20TH SETTING PERMITS MANUAL SELECTION OF ANY FREQUENCY WITHIN TUNING RANGE	SUPERHET	VOICE PULSE (WITH MODIFICATION)	5 UV	100 kc (1F)
R 807 ² R 808	0.2-1.5 2.0-18.0	AM	80 90 WATTS ¹	R-807 HF-10 PRESET ¹ LF-1 R-808 CONTINUOUS TUNING	SUPERHET	VOICE MORSE	5 UV	MINIMUM UNKN
R 809	30 70	FM	UNKNOWN	UNKNOWN	SUPERHET	PROBABLY VOICE ONLY	UNKNOWN	MINIMUM UNKN
R 814 ¹	100 150	AM	80 WATTS (EACH OF TWO TRANSMITTERS)	FOUR PRESET CHANNELS PER TRANSMITTER	R 801 RECEIVER R-808	VOICE MORSE POSSIBLY PULSE (WITH ADDITIONAL EQUIPMENT)	VHF SUV HF SUV	R 801 100 I (1F) R-808 MINIMUM UNK
R 820 ¹	0 2 0 55 3 18	AM FSK	600 W (VOICE) 100 W (MORSE) 1000 W (RTT)	UNKNOWN BUT SEE R-100	R 808, AMUR-11 ²	R-808 VOICE, MORSE AMUR-11 VOICE MORSE RTT VOICE RTT	R-808 5 UV AMUR-11 UNKNOWN	R 808 MINIM UNKNOWN
R 824 ¹	100 150	AM	400 W INTO ANTENNA	SIX PRESET CHANNELS ²	TWO R 800 OR R 801 RECEIVERS ²	VOICE PULSE (WITH ADDITIONAL EQUIP- MENT)	5 10 UV	100 kc (1F)
R 8K	100 150	AM	200 W	FOUR PRESET 601 RF CHANNELS AVAILABLE WITHIN FREQUENCY RANGE	SUPERHET	VOICE	5-10 UV	100 kc (1F)

1

SECRET

SECRET

FIG 15 (C) SOVIET COMMUNICATIONS. EQUIPMENT (CONT D)

NUMBER OF CHANNELS	RECEIVER TYPE	TYPE OF RECEPTION	RECEIVER SENSITIVITY	RECEIVER BANDWIDTH	RECEIVER SELECTIVITY	ANTENNA	INSTALLATION	REMARKS
	PROBABLY VOICE MORSE	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	UNKNOWN	VAN MOUNTED		REPORTEDLY IN USE FOR COMINT
AS ALTERNATIVE TO R 305								
3 kc INTERVALS	SUPERHET	VOICE PULSE (WITH ADDITIONAL EQUIPMENT)	5 10 UV	100 kc (1F)	ADJACENT CHANNEL REJECTION 10B	QUARTER-WAVE STUB	SOVIET FIGHTERS BOMBERS AND PROBABLY HELICOPTERS	FREQUENCY STABILITY (°) 10^{-3} ALTERNATE DESIGNATION RSIU 3M
1 CHANNELS Y REPORTED 601 AT 83.33 kc INTERVALS AVE ONLY 240 CH AT TERVALS	SUPERHET	VOICE PULSE (WITH ADDITIONAL EQUIP)	5 UV	100 kc (1F)	UNK	FLUSH	SOVIET FIGHTERS BOMBERS AND PROBABLY HELICOPTERS	FREQUENCY STABILITY (°) 10^{-3} ALTERNATE DESIGNATION RCIU 4
F TUNING RANGE. 100 kc INTERVALS SET TO SPECIFIC FRE WHILE 20TH SETTING ANUAL SELECTION OF ENCY WITHIN TUNING	SUPERHET	VOICE PULSE (WITH MODIFICATION)	5 UV	100 kc (1F)	UNKNOWN	FLUSH	MAY BE USED IN SOME FIGHTER BOMBER AIRCRAFT	FREQUENCY STABILITY (°) 10^{-4} ALTERNATE DESIGNATION OUB-5
10 PRESET ¹ LF-1 CONTINUOUS TUNING	SUPERHET	VOICE MORSE	5 UV	MINIMUM UNKNOWN	UNKNOWN	LONG WIRE	SOVIET BOMBERS, SOME FIGHTERS	1 R 807 (ALSO RSB-70) APPEARS TO BE COPY OF U.S. T-47 A-17-13 USED WITH R 808 (ALSO US-9) RECEIVER, WHICH IS SOVIET COPY OF U.S. BC-348 ELECTRICAL CHARACTERISTICS ARE ESTIMATED TO BE SIMILAR TO THESE U.S. EQUIPMENTS
	SUPERHET	PROBABLY VOICE ONLY	UNKNOWN	MINIMUM UNKNOWN	UNKNOWN	KULIKOV WHIP LONG WIRE	MAN PACK	
ET CHANNELS PER ER	R 801 RECEIVER R 808	VOICE MORSE POSSIBLY PULSE (WITH ADDITIONAL EQUIPMENT)	VHF 5UV HF 5UV	R 801 100 kc (1F) R 808 MINIMUM UNK	R 801	DISCONE PROBABLY ALSO YAGI	ZIL 151	1 ALTERNATE DESIGNATION RAS-SKP.
BUT SEE R-103	R 808. AMUR-11 ²	R 808 VOICE MORSE AMUR-11 VOICE MORSE RTT VOICE RTT	R 808 5 UV AMUR-11 UNKNOWN	R 808 MINIMUM UNKNOWN	UNKNOWN	WHIP DOUBLET LONG WIRE	ZIL-151	1 ALTERNATE DESIGNATION RAS-KVK 2 USE OF AMUR-11 REPORTED BUT EXAMINED STATION PROVIDED WITH UNKNOWN TYPE PROBABLY BOTH TYPES ARE UTILIZED
1 CHANNELS ²	TWO R 800 OR R 801 RECEIVERS ²	VOICE PULSE (WITH ADDITIONAL EQUIPMENT)	5 10 UV	100 kc (1F)	R 800 ADJACENT CHANNEL REJECTION 10B	DISCONE YAGI BROADBAND RECEIVER ANTENNA	ZIL-151	1 ALTERNATE DESIGNATION RAS-UKV 2 AN EXAMINED RAS-UKV (NO OTHER DESIGNATION), HOWEVER HAD ONLY FOUR PRESET, PUSHBUTTON FREQUENCIES IT IS POSSIBLE THAT R-824 APPLIES ONLY TO A SIX-CHANNEL VERSION OF THE RAS-UKV AND THAT THE EXAMINED STATION WOULD HAVE ANOTHER R 800 SERIES NUMBER. THE EXAMINED STATION HAD R-800 RECEIVERS
ET 601 RF CHANNELS WITHIN FREQUENCY	SUPERHET	VOICE	5-10 UV	100 kc (1F)	UNKNOWN	DISCONE, PROBABLY ALSO YAGI	MOBILE STATION	

2

SECRET

FIG 16 - U S JAMMING EQUIPMENT

EQUIPMENT	COGNIZANT SERVICE	FREQUENCY (Mc)	FUNCTIONAL DESCRIPTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	
AN/ALQ-33	USN	50-200	AIRBORNE, AUTOMATIC TUNING RECEIVER AND AUTOMATIC TUNING TRANSMITTER TO PROVIDE A DEFENSE AGAINST COMMUNICATIONS, RADAR, OR GUIDED MISSILE CONTROL SIGNALS, CW, OR PULSED	BROADBAND NOISE, CW, OR SINE WAVE TONE FM MODULATION	RF-BARRAGE AND SHOT CLASS EMISSION. USES 4 x 150'S	BLADE TYPE AS 926/ALQ-33	AM I MATII HETE; WICHT
AN/ALT-3	USAF	2-28 (10-BANDS)	AIRBORNE COMMUNICATIONS JAMMER CHARACTERIZED BY RANDOM NOISE AM AND RANDOM RATE FREQUENCY SWEEP WHICH PRODUCES A SIMULTANEOUS INTERFERENCE WITH ALL SIGNALS WITHIN ITS FREQUENCY RANGE.	NOISE AM AND CW SWEPT; RANDOM RATE SWEEP 400-600 cps	4 EA 4 x 150 USED FOR OUTPUT	PROPOSED 22 FT WIRE ANTENNA ALONG ACFT BOTTOM SAME AS FOR AN ARC-21 RADIO	NONE PLUG BAND
AN ALT-7	USAF	24-352 (2 TRANS-MITTERS) 24-170, 168-352	SWEPT AND SPOT NOISE JAMMER FOR USE AGAINST VHF AND UHF, GCI & EW RADARS	CW FOR SPOT JAMMING OR NOISE-MODULATED AM FOR BARRAGE JAMMING SWEEP RATE 8-400 cps 2-4 Mc NOISE CW MODULATION, ALSO FM SWEEP BANDWIDTH OF 10% OF TRANSMITTER CENTER FREQ	T-464 ALT-7 T-465 ALT-7	2 REQUIRED. ONE FOR EA TRANS-MITTER BUT NOT SUPPLIED	NONE SEARC RE-QL
AN ALT-12 (XY 1)	USAF	50-350 IN TWO BANDS 50-130 130-350	WIDE BAND BARRAGE JAMMING SYSTEM USED AS A MEANS FOR DISABLING A MULTIPLE NUMBER OF EARLY WARNING RADARS	AM NOISE MODULATION FROM AN INTERNAL SOURCE CW PULSED CW, OR A MODULATED CW SIGNAL MAY BE SUPPLIED FROM AN EXTERNAL SOURCE	2 TRANSMITTERS, 1 LOW BAND AND 1 HIGH BAND, UTILIZES DISTRIBUTED AMPLIFIERS	4 ANTENNAS 2 LOW BAND AT 600 50-90 Mc. AT-190B 90-130 Mc 2 HIGH BAND AT-191B AP 130-200 Mc AT 183B/AP 200-350 Mc	
AN ARC 1 1X 1A 1AX	USN	100-156 IN 9 PRESET CH. GUARD CHAT 121.5	AIRBORNE EQUIPMENT NORMALLY USED AS A RECEIVER-TRANSMITTER FOR AM MODULATED SIGNALS, BUT IS SOMETIMES EMPLOYED AS A JAMMER. COVERS THE FREQUENCY BANDS IN 9 PRESET CONTROLLED BANDS, ANY OF WHICH CAN BE SELECTED BY THE PILOT. GUARD CHANNEL PERMITS MONITORING	AMPLITUDE	INTEGRAL PART OF EQUIPMENT RT-18 ARC-1 OR RT-18A ARC-1	AT-8R AR STUB ANTENNA OR ROD TYPE OR MAST TYPE	INTEG EQUIP 9.72 TIVIT VOLTS CIRCU NOISE AUDIO
AN ARC 27 27A	USN USAF	225-399.9 IN 1750 CH 100 kc APART 238-248 Mc GUARD CHAN	THIS EQUIPMENT WAS DESIGNED PRIMARILY TO PROVIDE A 2-WAY AMPLITUDE-MODULATED VOICE RADIO TELEPHONE COMMUNICATIONS BETWEEN ACFT INFLIGHT, ACFT AND SHIP, OR ACFT AND SHORE STATION, BUT HAS BEEN EMPLOYED AS A JAMMER	AMPLITUDE, 90-95% BY VOICE OR A 1020 cps TONE TONE MAY BE USED FOR EMERGENCY OF PURPOSES	INTEGRAL PART OF EQUIP -0 005 FREQ STABILITY 50 OHMS OUTPUT IMPEDANCE 8 SEC MAX CH SELECTION 100 MILLISECOND TRANSMIT RECEIVE INTERVAL	AT-141 ARC RE-QUIRED AT 256 ARC SLEEVE USED FOR TESTING IN TF 10 ACFT	FREQ -0 00 VITY SELEC BAND 1 db AI OUTPUT DISTOI MAX
AN ARQ 8	USN USAF	25-105	AIRBORNE RADIO TRANSMITTING AND RECEIVING SET WHICH PROVIDES A NOISE-MODULATED SIGNAL FOR JAMMING ENEMY RADIO COMMUNICATIONS AND RADAR SYSTEMS. EITHER SPOT OR BARRAGE TYPE JAMMING MAY BE UTILIZED WITH INTERCHANGEABLE PREAMP STRIPS	NOISE MODULATED, EITHER SPOT OR BARRAGE JAMMING MAY BE USED BY INTERCHANGING PREAMP STRIPS AS AM-22A/ARQ-8, BAND WIDTH 100 kc-SPOT AM 23A ARQ-8 BANDWIDTH 4 Mc-BARRAGE	T-51A ARQ-8 TRANSMITTER T-51B ARQ-8 MODIFIED UNIT	LOW END FREQ FAN TYPE 1 HIGH END WHIP TYPE, 4 RECEIVING WIRE TYPE	R 58A
AN ARQ 10	USN	165 kc-80 Mc COVERED BY 3 RF HEADS. ONLY ONE CAN BE USED AT A TIME	AIRBORNE SPOT FREQUENCY JAMMER IT CAN BE USED AS A COMMUNICATIONS EQUIPMENT BOTH FOR TELEPHONE AND TELEGRAPHY	AM RESISTANCE NOISE SOURCE WITH BANDWIDTH LIMITED TO 6 kc OR WOBBLATOR FROM 500-1200 cps AT A RATE APPROX 2 PER SECOND OR FROM EXTERNAL SOURCE FM AUDIO 250 cps NARROW DEVIATION 200 cps WIDE DEVIATION DEPENDS ON CARRIER FREQ MAX 16 kc AT 80 Mc	RT-50 ARQ-10 RT-51 ARQ-10 RT-52 ARQ-10	TRANSMITTER IMPED 50 OHMS RCVR IMPED 50 OHMS ROTATE AT 4800 rpm NOMINAL	INTEGI 3 RF I TIVIT VOLTS 130 k 569 5 3020 1

1

SECRET

SECRET

FIG 16 - U S JAMMING EQUIPMENT

FUNCTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	RECEIVER	POWER OUTPUT AND POWER REQUIRED	LOOK THRU	REMARKS
3 RECEIVER SMITTER TO COMMUNI- MISSILE JLSED	BROADBAND NOISE, CW, OR SINE WAVE TONE FM MODU- LATION	RF-BARRAGE AND SHOT CLASS EMISSION. USES 4 x 150'S	BLADE TYPE AS 926/ALO-33	AM PULSE AUTO- MATICALLY TUNED. HETERODYNE BAND- WIDTH ±75	OUTPUT 200 WATTS MAXIMUM REQUIRED 1200 WATTS, 115V, 320- 1760 cps, 3 PHASE, AND 100W, 115V, 320-420 cps, SINGLE PHASE	RANDOM	PRODUCTION N600(A), 43035
MMER ISE AM SWEEP OUS IALS WITHIN	NOISE AM AND CW SWEPT; RANDOM RATE SWEEP 400- 600 cps	4 EA 4 x 150 USED FOR OUTPUT	PROPOSED 22 FT WIRE ANTENNA ALONG ACFT BOTTOM SAME AS FOR AN/ARC-21 RADIO	NONE TUNING 3- PLUG-IN UNITS PER BAND	OUTPUT 150W NOMINAL 60-250 WATTS REQUIRED 1650W, 115V, 380-420 cps 3 PHASE (WYE) AND 0.9 AMPS, 28 VDC	UNK	PRODUCTION AF 33(600) 25237 (CLOSED)
R FOR USE EW RADARS	CW FOR SPOT JAMMING OR NOISE-MODULATED AM FOR BARRAGE JAMMING SWEEP RATE 8-400 cps 2-4 Mc NOISE CW MODULATION, ALSO FM SWEEP BANDWIDTH OF 10% OF TRANSMITTER CENTER FREQ	T-464/ALT-7 T-465/ALT-7	2 REQUIRED, ONE FOR EA TRANS- MITTER BUT NOT SUPPLIED	NONE ASSOCIATED SEARCH RECEIVER RE-QUIRED	OUTPUT T-464 ALT-7, 70 WATTS T 465 ALT-7 100 WATTS, 150 WATTS MAXIMUM REQUIRED 1500 VA, 115V 380-1000 cps, SINGLE PHASE 250W 28 VDC	PANORAMIC INDICATOR MUST BE USED, RANDOM	PRODUCTION AF 33(600) 23495 (SEE ORC-18(T) FOR AN ALT-7 MODIFI- CATIONS)
SYSTEM ING A ARNING	AM NOISE MODULATION FROM AN INTERNAL SOURCE CW PULSED CW, OR A MODULATED CW SIGNAL MAY BE SUPPLIED FROM AN EXTERNAL SOURCE	2 TRANSMITTERS, 1 LOW BAND AND 1 HIGH BAND, UTILIZES DISTRI- BUTED AMPLIFIERS	4 ANTENNAS 2 LOW BAND AT 600 50-90 Mc, AT-190B 90-130 Mc, 2 HIGH BAND AT-191B/AP 130-200 Mc AT- 183B/AP 200-350 Mc		OUTPUT CAPABLE OF BEING PRESET FROM 0-1 SW PER MEGACYCLE LOW BAND 120W HIGH BAND 330W, REQUIRED 6200VA, 115V 400 cps 3 PHASE		SERVICE TEST AF 33(604) 16289
Y USED AS AM MODU- TIMES RS THE CON- CAN BE D CHANNEL	AMPLITUDE	INTEGRAL PART OF EQUIPMENT RT-18 ARC-1 OR RT-18A ARC 1	AT-8R AR STUB ANTENNA OR ROD TYPE OR MAST TYPE	INTEGRAL PART OF EQUIPMENT IF 9.72 Mc SENSITIV- ITY 2.8 MICRO- VOLTS SQUELCH CIRCUIT AND PEAK NOISE LIMITER FOR NOISE SUPPRESSION AUDIO OUTPUT	OUTPUT 8 WATTS BANDWIDTH, -25 db DOWN AT 100 kc FROM RESONANCE REQUIRED 450W, 115 OR 230V, 60 cps, SINGLE PHASE 7.5 AMPS MAX INTER- MITTANT AT 26 VDC		PRODUCTION NXsa 31225 (ARC-1-1X) NXsa 96346(1A, -1AX)
3 PRI- AMPLITUDE- PHONE IN FLIGHT SHORE YED AS A	AMPLITUDE, 90-95% BY VOICE OR A 1020 cps TONE TONE MAY BE USED FOR EMERGENCY OF PURPOSES	INTEGRAL PART OF EQUIP -0.005 FREQ STABILITY 50 OHMS OUTPUT IMPEDANCE, 8 SEC MAX CH SELECTION 100 MILLISECOND TRANSMIT RECEIVE INTERVAL	AT-141 ARC RE- QUIRED AT 256/ARC SLEEVE USED FOR TESTING IN TF 10 ACFT	FREQ STABILITY, -0.005% SENSITI- VITY 5 MICROVOLT SELECTIVITY 85 kc BAND WIDTH AT 6- db AUDIO POWER OUTPUT 0.5W AUD DISTORTION 15% MAX	OUTPUT 9 WATTS REQUIRED, 25.5 AMPS MAXIMUM AT 27 VOLTS dc		PRODUCTION NOa(s) 51-284 NObsr 30119
3 AND S A NOISE IG ENEMY IDAR IRAGE TYPE H INTER	NOISE MODULATED EITHER SPOT OR BARRAGE JAMMING MAY BE USED BY INTER- CHANGING PREAMP STRIPS AS AM-22A ARQ-8, BAND WIDTH 100 kc SPOT AM 23A ARQ-8 BANDWIDTH 4 Mc-BARRAGE	T-51A ARQ-8 TRANSMITTER T-51B ARQ-8 MODIFIED UNIT	LOW END FREQ FAN TYPE 1 HIGH END WHIP TYPE, 4 RECEIVING WIRE TYPE	R 58A ARQ-8	OUTPUT 30 WATTS, REQUIRED TRANS- MITTER -350W, 80-115V, 400-2600 cps SINGLE PHASE, 1-AMP, 28 VDC RECEIVER 55W 80-115V, 400-2600 cps SINGLE PHASE	6 UNITS MODIFIED TO SHOW IF SIG IS BEING JAMMED	PRODUCTION COMPLETE 696-DAV-44 MODIFI- CATION AF 33 (600) 26117 CALL NO 2
MMER IT IONS Y AND	AM RESISTANCE NOISE SOURCE WITH BANDWIDTH LIMITED TO 6 kc OR WOBBLATOR FROM 500-1200 cps AT A RATE APPROX 2 PER SECOND OR FROM EX- TERNAL SOURCE FM AUDIO 250 cps NARROW DEVIATION 200 cps WIDE DEVIATION DEPENDS ON CARRIER FREQ MAX 16 kc AT 80 Mc	RT-50 ARQ-10 RT-51 ARQ-10 RT-52 ARQ-10	TRANSMITTER IMPED- 50 OHMS RCVR IMPED-50 OHMS ROTATE AT 4800 rpm NOMINAL	INTEGRAL PART OF 3 RF UNITS SENSITIV- ITY 20 MICRO- VOLTS IF UNIT L 130 kc UNIT M 569.5 kc UNIT N 3020 kc	OUTPUT UNIT L 30 WATTS Z UNIT M AND N 50 WATTS REQUIRED, 700 VA 115V 400-2400 cps SINGLE PHASE 10 AMPS 26 VDC		PRODUCTION NXsa 42137

2

SECRET

SECRET

FIG 16 - U S JAMMING EQUIPMENT (CONT'D)

EQUIPMENT	COGNIZANT SERVICE	FREQUENCY (Mc)	FUNCTIONAL DESCRIPTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	
AN GLQ-2	USA	1 5-20 Mc IN 4 BANDS 1 5-2 9, 2 9-5 0, 5 0-10 0, 10-20	GROUND-BASED TRANSPORTABLE EQUIP. PRIMARILY USED FOR SPOT JAMMING OF ENEMY RADIO COMMUNICATIONS. IF TRUCK MOUNTED, EQUIPMENT CAN BE OPERATED WHILE THE VEHICLE IS IN MOTION. AVERAGE TIME REQUIRED TO TUNE THE EQUIPMENT TO A NEW VICTIM SIGNAL IS 193-SECONDS	NARROW BAND FM (STEP TONES & VOICE AND NOISE) RANDOM CW AND KEYED CW FM BAND-WIDTH - 6 kc AM BANDWIDTH- 7 kc	RT 260-GLQ-2 FEEDS OUTPUT TO TRANSMITTER T-368 URT WHERE SUFFICIENT POWER IS PROVIDED FOR JAMMING	4 WHIP ANT. 2 FOR RECEIVING, 1 TRANSMITTING & OR RCVG SEMI-FIX cps END-FED LONG WIRE FOR SENDING & RECEIVING 1 4-6 4 Mc	RT-REC NAL IF- TIV VOL WID
AN GLQ-3	USA	20-230 IN SEVEN BANDS	GROUND TRANSPORTABLE ASSEMBLY OF ELECTRONIC EQUIPMENT USED TO JAM ENEMY COMMUNICATIONS EQUIPMENT. POSSIBLE USE MAY BE MADE AGAINST RADAR AND NAVIGATIONAL EQUIPMENT. IT SPOT JAMS AM, FM OR CW RECEIVING EQUIPMENTS. ONE OPERATOR IS REQUIRED.	TRANSMITS AM, FM, COMBINATION OF AM & FM, CW & PULSE MODULATING SOURCES ARE VOICE, NOISE, CONTINUOUS TONE, KEYED TONE, STEPPED TONE, SAW AND OTHER EXTERNALLY GENERATED SIGNALS AND COMBINATIONS THEREOF	INTEGRAL PART OF AN-GLQ-3 (XE-1)	AT-318/TLR-60-230 Mc, AT-605(XE-1) 60-150 Mc, AT-608(XE-1) 140-230 Mc, AT-744 (XE-1) 20-81 Mc, AS-877 (XE-1) 20-57 Mc	R-2 FIE AUT EXC
AN W1Q-22 (XE-1)	USA	6-10, 500	MULTIPURPOSE, TRUCK-MOUNTED SPOT JAMMER WITH CHOICE OF AM, FM, OR PULSE OUTPUT. THIS SYSTEM IS CAPABLE OF TRANSMITTING FOUR SIMULTANEOUS JAMMING SIGNALS. THIS SYSTEM IS MADE UP OF RECEIVING SETS, DIRECTION FINDING EQUIP., ANALYZING EQUIP., JAMMERS AND ANTENNA GROUPS.	AM FM OR PULSE, CW	AN/TLT-1 1 EACH AN/TLT-2 1 EACH AN/TLT-2 2 EACH 1 EA UNIT TO COVER 285-350 Mc BANDS.	INFLATABLE MONOPOLE (6-19 Mc) INFLAT MONOPOLE (20-56 Mc) LOG PERIODIC 56-285 NELICES & HORNS 285-10, 500 Mc	MANI MAT
AN SPT-1	USN	93-210	SHIPBORNE, COUNTERMEASURES TRANSMITTING SYSTEM FOR JAMMING RADAR SIGNALS IN THE VHF RANGE.	AM EMISSION WITH A 5 Mc BANDWIDTH, AM MODULATED WITH ONLY ONE SIDEBAND USED WITH THE CARRIER SUPPRESSED NOISE MODULATED.	T-28/APT-1	3 QUARTER WAVE STUBS	NONE
AN SPT-3	USN	89-136 WITH 829 AMPLIFIER 105-154 5 WITH 832 AMPLIFIER	SHIPBORNE, NOISE-MODULATED, BARRAGE-TYPE COUNTERMEASURES TRANSMITTER FOR JAMMING RADAR SIGNALS IN THE VHF RANGE. TWO MAY BE OPERATED SIMULTANEOUSLY WITH THE ONE GENERATOR FURNISHED WITH THE EQUIPMENT	AM NOISE-MODULATED; CARRIER SIDE BAND ± 3 Mc	T-27/APT-3	AP-37/APT AP-38/APT QUARTER-WAVE STUBS	NONE
AN TLQ-15	USA	1 5-20 Mc IN 5 BANDS WITH 5% OVERLAP	GROUND-TRANSPORTABLE COMMUNICATIONS JAMMER WHICH CAN BE TRUCK MOUNTED AND OPERATED ON THE UPPER BANDS WHILE THE VEHICLE IS IN MOTION	DRIVING SIGNAL MODULATED	INTERMEDIATE RF AMPLIFIER AND FINAL RF AMPLIFIER DRIVEN BY HF JAMMER EXCITER UNIT INPUT VOLTAGE IS FROM 0-10	1-15 FT WHIP 1-30 FT WHIP	SUPE IF R db, ION, WIDT 6 db
MAS	USN	41-51	THE MAS COUNTERMEASURES JAMMING EQUIPMENT INCORPORATES A RECEIVER WITH LOOK-THRU PROVIDED CW OR AUDIO MODULATION OF 1, 1 5, 8, OR 12 MAY BE USED	1000 1500, 8000 OR 12 000 cps MODULATION FREQUENCY INTERRUPTED 10 TIMES PER SECOND	NOT GIVEN	NOT GIVEN	RESPI ESSE BETW AND !
TDY	USN	175-770	THE TDY IS DESIGNED PRIMARILY FOR SHIPBOARD JAMMING USE. THE TRANSMITTER RADIATES A RANDOM NOISE MODULATED SIGNAL. A SEPARATED RECEIVER MUST BE PROVIDED	MCW AM, NOISE	NOT GIVEN	NOT GIVEN	NOT C
TDY-1	USN	115-770	THE TDY-1 IS DESIGNED FOR SHIPBOARD INSTALLATION. ITS PURPOSE IS TO RADIATE A WIDE BAND JAMMING SIGNAL OF A CARRIER FREQUENCY EMPLOYED BY ENEMY COMMUNICATIONS OR RADAR SYSTEMS TO RENDER THE EQUIPMENT INOPERATIVE. A SEPARATE RECEIVER MUST BE FURNISHED	WIDE BAND RANDOM NOISE	NOT GIVEN	NOT GIVEN	

1

SECRET

SECRET

FIG 16 - U S JAMMING EQUIPMENT (CONT'D)

FUNCTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	RECEIVER	POWER OUTPUT AND POWER REQUIRED	LOOK THRU	REMARKS
EQUIPMENT JAMMING OF IF TRUCK OPERATED ATION AVER EQUIPMENT 193-	NARROW BAND FM (STEP TONES & VOICE, AND NOISE) RANDOM CW AND KEYED CW FM BAND- WIDTH - 6 kc AM BANDWIDTH- 7 kc	RT 260/GLQ-2 FEEDS OUTPUT TO TRANSMITTER T- 368/URT WHERE SUFFICIENT POWER IS PROVIDED FOR JAMMING	4 WHIP ANT 2 FOR RECEIVING, 1 TRANSMITTING & OR RCVG SEMI- FIX cps END-FED LONG WIRE FOR SENDING & RE- CEIVING 1.4-6.4 Mc	RT-260/GLQ-2 & RECEIVES AM SIG- NALS FOR JAMMING IF-465 kc, SENSITIVITY-5 MICRO- VOLTS, IF BAND- WIDTH, 6 kc	AVERAGE POWER OUTPUT: 450W, FM 657W, AM REQUIRED, 115-125V, 60 cps, SINGLE PHASE, SUPPLIED BY PE-95 POWER UNIT.	PROVIDED MOD KITS & VARIES	PRODUCTION DA 36-039 SC6996 DA 36-039 SC75283 DA 36-039 SC72367 DA 36-039 SC66483
BLY OF TO JAM MENT. GAINST PMENT IT EIVING S REQUIRED.	TRANSMITS AM, FM, COMBI- NATION OF AM & FM, CW & PULSE MODULATING SOURCES ARE VOICE, NOISE, CON- TINUOUS TONE, KEYED TONE, STEPPED TONE, SAW AND OTHER EXTERNALLY GENERATED SIGNALS AND COMBINATIONS THEREOF	INTEGRAL PART OF AN/GLQ-3 (XE-1)	AT-318/TLR-60-230 Mc, AT-605(XE-) 60-150 Mc, AT- 608(XE-) 140-230 Mc, AT-744 (XE-1) 20-81 Mc, AS-877 (XE-1) 20-57 Mc	R-220/URR, MODI- FIED TO PROVIDE AUTOMATIC EXCITATION	OUTPUT: 100-150 WATTS NOMINAL, REQUIRED: 2480W OR 23.3 AMPS AT 115V, 50-60 cps, SINGLE PHASE.	VISUAL DISPLAY ON IP-418 (XE-1)/GLQ-3	SERVICE TEST DA 36-039 SC-36611
D SPOT FM, OR IS CAPABLE TANEOUS EM IS MADE CTION QUIP.	AM FM OR PULSE, CW	AN/TLT-1 1 EACH AN/TLT-2 1 EACH AN/TLT-2 2 EACH 1 EA UNIT TO COVER 285-350 Mc BANDS.	INFLATABLE MONO- POLE (6-19 Mc) INFLAT MONOPOLE (20-56 Mc) LOG PERIODIC 56-285 NELICES & HORNS 285-10.500 Mc	MANUAL AND AUTO- MATIC	OUTPUT: AVERAGE 150 WATTS, REQUIRED: 115V, 60 cps, SINGLE PH, 115V, 400 cps, 3 PHASE AND 28 VDC.		DEVELOPMENT, LIMITED PRODUCTION DA 36-039 SC-78166
TRANS- RADAR	AM EMISSION WITH A 5 Mc BANDWIDTH, AM MODULATED WITH ONLY ONE SIDEBAND USED WITH THE CARRIER SUPPRESSED NOISE MODULATED.	T 28/APT-1	3 QUARTER WAVE STUBS	NONE	OUTPUT: 13W, AT 93 Mc TO 6W AT 210 Mc. A SPECIAL TUBE 829B MAY BE USED TO INCREASE OUTPUT TO 28W AT 93 Mc AND 16W AT 162 Mc. REQ.: 80-115V, 400-2800 cps, SINGLE PH; 115V, 60 cps, 1 PH; 115 VDC.		PRODUCTION NXss-33626
BARRAGE- FITTER FOR IE VHF SIMUL- RATOR IT	AM NOISE-MODULATED; CARRIER SIDE BAND ± 3 Mc	T-27/APT-3	AP-37/APT AP-38/APT QUARTER-WAVE STUBS	NONE	OUTPUT: 9 0-14.8W WITH 832 AMPLIFIER, 7.5-16.0W WITH 829 AMPLIFIER. RE- QUIRED: 600W AT 105-125V, 500 cps, SINGLE PH AND 100 WATTS AT 26 VDC.		PRODUCTION NXss-33626
ICATIONS OUNTED AND WHILE THE	DRIVING SIGNAL MODULATED	INTERMEDIATE RF AMPLIFIER AND FINAL RF AMPLIFIER DRIVEN BY HF JAM- MER EXCITER UNIT INPUT VOLTAGE IS FROM 0-10	1-15 FT WHIP 1-30 FT WHIP	SUPERHETERODYNE IF REJECTION 60- db, IMAGE REJECT- ION, 60 db, BAND- WIDTH, 6 kc AT 6 db DOWN POINTS	OUTPUT: 2 kw AVERAGE; BANDWIDTH 100- 3500 cps ± 1 db. SWITCHING IS PROVIDED FOR OPERATING AT REDUCED POWER RE- QUIRED: 12.5 kw, 208V $\pm 5\%$, 400 cps, SINGLE PHASE. POWER SOURCE PU-107/L		DEVELOPMENT SERVICE TEST DA 36-039 SC78026
NING EQUIP- R WITH UDIO 12 MAY	1000 1500, 8000 OR 12 000 cps MODULATION FREQUENCY INTERRUPTED 10 TIMES PER SECOND	NOT GIVEN	NOT GIVEN	RESPONSE IS ESSENTIALLY FLAT BETWEEN 500 cps AND 50 kc	OUTPUT: CW 150W OR MCW 250W REQUIRED, 10 AMPS, 115V, 60 cps, SINGLE PHASE.	PROVIDED AT 10 cps RATE	PRODUCTION AIL
LY FOR TRANSMITTER JLATED R MUST BE	MCW, AM, NOISE	NOT GIVEN	NOT GIVEN	NOT GIVEN	OUTPUT: 150 WATTS NOMINAL, REQUIRED 2 kva AT 105-125V 57-63 cps, SINGLE PHASE, 2 kva, 210-250 OR 420-500V, 57-63 cps, SINGLE PHASE.		PRODUCTION COMPLETED NXsr 3803
IPBOARD S TO RADIAL OF A Y ENEMY TENS TO TIVE A IRNISHED	WIDE BAND RANDOM NOISE	NOT GIVEN	NOT GIVEN		OUTPUT: 150 WATTS REQUIRED 2-kva, 115V, 60 cps SINGLE PHASE		PRODUCTION COMPLETED NXsr 48345

2

SECRET

SECRET

FIG 16 - U.S. JAMMING EQUIPMENT (CONT'D)

EQUIPMENT	COGNIZANT SERVICE	FREQUENCY (Mc)	FUNCTIONAL DESCRIPTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	
MD-150(XN-1) SRT MD-150 SRT	USN	PROVIDES AUDIO MODULATION	SHIPBOARD COMMUNICATIONS JAMMING SET PROVIDES VARIOUS MODULATION SIGNALS FOR STANDARD COMM TRANSMITTERS AND HAS RECORDERS FOR DECEPTION PLAYBACK ONE OPERATOR & IS PRIMARILY DESIGNED FOR USE IN CONJUNCTION WITH TRANSMITTER URT-4.	BAG PIPE, NOISE, SAW, RANDOM SAW, FAX, AND TTY. NOTE: ANY SIGNAL GENERATED WITHIN MODULATOR FROM AN EXTERNAL SOURCE CAN BE RECORDED & PLAYED BACK. MULTI-RECORDINGS OF TWO OR MORE SIGNALS CAN BE MADE AND PLAYED BACK.	NOT GIVEN	NOT GIVEN	
QRC-4(T)	USAF	100-156	THESE EQUIPMENTS PROVIDE AN AUTOMATIC METHOD OF DETECTING AND JAMMING GROUND AND AIRBORNE SIGNALS BEING USED AGAINST THE ACFT IN WHICH THE EQUIPMENT IS INSTALLED. THE EQUIPMENT TRANSMITS A PULSE OF ENERGY AT THE RECEIVED FREQUENCY EACH TIME A SIGNAL IS RECEIVED.	EQUIPMENT AUTOMATICALLY TRANSMITS A PULSE OF ENERGY AT THE RECEIVED FREQUENCY EACH TIME A SIGNAL IS RECEIVED.	AUTOMATIC SCANNING, PRF 200-2000 cps, BANDWIDTH 1-4 Mc	NOT GIVEN	INT. EQL TO TIF APP TRA SHL
QRC-8(T)	USAF	2-10	FREQUENCY-SWEPT CW COMMUNICATIONS JAMMER WAS BUILT AROUND A REDESIGNED HF JAMMING TRANSMITTER	CARRIER SWEPT	HF JAMMING TRANSMITTER REMOTELY CONTROLLED BY "ON-OFF" SWITCH	NOT GIVEN	
QRC-13(T)	USAF	JAMMERS 2-18.1 24-352	THIS WAS SUPPOSED TO BE AN INTERIM GROUND BASED ECM SYSTEM WHICH PROVIDES FOR A LIMITED PASSIVE DETECTION AND COMMUNICATIONS JAMMING CAPABILITY FOR TAC. THIS FACILITY WILL BE EMPLOYED AS A PART OF THE TACTICAL CONTROL SYSTEM AND WILL PROVIDE A LIMITED CAPABILITY FOR THE FOLLOWING FUNCTIONS: RADAR ALERTING, RADAR ASSISTING, COMMUNICATIONS JAMMING, AND INTELLIGENCE. THE SYSTEM IS COMPOSED OF THREE IDENTICAL, SELF-CONTAINED, SELF-PROPELLED UNITS. EACH UNIT INCORPORATES 8 MAIN EQUIPMENT GROUPS, ONE OF WHICH IS THE COMM JAMMING GROUP: JAMS BY NOISE, CW, AM, OR FM SIGNALS.	NOISE, CW, AM, OR FM SIGNALS. FM SWEEP 10% OF CENTER FREQ & MOD FREQ IS 0-400 cps, ON ART-13A. NOISE PRODUCED BY EXTERNAL NOISE MODULATOR. ON T-465 CW, AND FM HAS SWEEP RANGE 7-10% OF CENTER FREQUENCY FROM LOW TO HIGH END OF BAND.	T-464, ALT-7 24-170 Mc T-465, ALT-7 168-352 Mc AN ART-13A 2-18.1 Mc	AT-546 (24-100 Mc) AS-541 (75-170 Mc) AT-197 GR (168-352 Mc) AN ART 13A-75 FT WIRE AT-544 (0.55 Mc-42 Mc) AT-543 (38-135 Mc) AT-545 (125-300 Mc)	AN Mc AN Mc AN Mc ARR UHF SCA (70 BAN)
QRC-22(T)	USAF	50-90	AIRBORNE VHF JAMMER, A NOISE BARRAGE JAMMER CAPABLE OF AMPLIFYING AND TRANSMITTING RANDOM RF NOISE	NOISE POWER RF RANDOM NOISE FROM INTERNAL NOISE GENERATOR OR OTHER TYPE RF SIGNALS FROM EXTERNAL SOURCES	TUNED BYPASS AMPLIFIERS DRIVEN BY AN INTERNAL NOISE SOURCE	2 MODIFIED AS 161 ART WHIP ANTENNAS, VSWR OVER ENTIRE BAND IS LESS THAN 7:1 AND NEAR MID FREQ IS LESS THAN 3:1	
QRC-65(T)	USAF	95-160 APPROX AT 3:1 VSWR	A SWEPT ECM SYSTEM IN THE VHF FREQUENCY RANGE WHICH BOTH RECEIVES AND JAMS A TARGET. THIS EQUIPMENT PROVIDES A MEANS FOR MAKING COMMUNICATIONS SIGNALS.	AM-FM NOISE MODULATIONS	SWEPT, HAS FREQUENCY LOCK-ON FEATURE TWO 4 x 250 s, ONE SECOND JAMMING TIME	MODIFIED AT-190-B	SWEPT 2 MI TO d NOIS SUPE BAND
VHF COMMUNICATIONS JAMMER (CGS LABS)	USN	100-156	A COMMUNICATIONS JAMMER WHICH SWEEP-RECEIVES AND TRANSMITS ACROSS THE FREQUENCY BAND IN FIVE CHANNELS. THE EQUIPMENT MAKES USE OF VARIABLE RECTIFIERS AND HAS A 400 MICROSECOND SET-UP CYCLE.	NOT GIVEN	DIVIDED INTO 5 CHANNELS STOPS 2.5 SECONDS ON FREQUENCY TO BE JAMMED	UNKNOWN	SWEP
AN APQ-2	USN	200-550 Mc WITH MOD KIT FOR FM RANGE STARTS AT 150 Mc	AIRBORNE TRANSMITTER DESIGNED TO JAM COMMUNICATIONS SYSTEMS. JAMS WITH AN AM TYPE EMISSION USUALLY FM MODULATION MAY BE UTILIZED WITH A MODIFICATION KIT.	AM WITH NOISE, 6 Mc BANDWIDTH, FM WITH NOISE IN THE RF FREQUENCY RANGE OF 150-350 Mc WITH THE USE OF MODIFICATION KIT MX-527 APQ-2	T 9 APQ 2	NOT KNOWN	NONE

1

SECRET

SECRET

FIG 1G - U.S. JAMMING EQUIPMENT (CONT'D)

CTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	RECEIVER	POWER OUTPUT AND POWER REQUIRED	LOOK THRU	REMARKS
JAMMING SET ON SIGNALS ITTERS AND ON PLAYBACK LY DESIGNED TH TRANS-	BAG PIPE, NOISE, SAW RANDOM SAW, FAX, AND TTY NOTE ANY SIGNAL GENERATED WITHIN MODULATOR FROM AN EXTERNAL SOURCE CAN BE RECORDED & PLAYED BACK MULTI-RECORDINGS OF TWO OR MORE SIGNALS CAN BE MADE AND PLAYED BACK	NOT GIVEN	NOT GIVEN		REQUIRED 172 VA 115V 60 cps SINGLE PHASE		PRODUCTION DUMONT
AN AUTOMATIC AMMING LS BEING WHICH THE HE EQUIPMENT BY AT THE TIME A SIGNAL	EQUIPMENT AUTOMATICALLY TRANSMITS A PULSE OF ENERGY AT THE RECEIVED FREQUENCY EACH TIME A SIGNAL IS RECEIVED.	AUTOMATIC SCANNING, PRF 200-2000 cps BANDWIDTH 1-4 Mc	NOT GIVEN	INTEGRAL PART OF EQUIP LOCKS ON TO FREQUENCY AND TIMES TRANSMITTER IF SIGNAL DISAPPEARS, THE TRANSMITTER IS SHUT OFF	OUTPUT PEAK POWER - 10 kw PULSE-WIDTH ADJUSTABLE, 10-70 MICROSECONDS DUTY CYCLE-EMITS PULSE WHEN SIGNALS IS RECEIVED REQUIRED UNK		PRODUCTION COMPLETED PROGRAM ABANDONED DUE TO POOR FLIGHT RESULT
ICATIONS REDESIGNED	CARRIER SWEPT	HF JAMMING TRANSMITTER REMOTELY CONTROLLED BY "ON-OFF" SWITCH	NOT GIVEN		REQUIRED A MODIFIED RECTIFIER POWER UNIT-PP-87 APT-4 IS USED IN CONJUNCTION WITH TRANSMITTER		PRODUCTION COMPLETED AF 33(600) 26117
4 INTERIM HIGH PRO-E DETECTION CAPABILITY L BE EM-ICTICAL CONDE A FOLLOWING RADAR JAMMING, EM IS COM-SELF-CONTS EACH EQUIPMENT E COMM SE, CW, AM.	NOISE, CW, AM, OR FM SIGNALS FM SWEEP 10% OF CENTER FREQ & MOD FREQ IS 0-400 cps, ON ART-13A NOISE PRODUCED BY EXTERNAL NOISE MODULATOR ON T-465 CW, AND FM HAS SWEEP RANGE 7-10% OF CENTER FREQUENCY FROM LOW TO HIGH END OF BAND	T-464, ALT 7 24-170 Mc T-465, ALT-7 168-352 Mc AN ART-13A 2-18 1 Mc	AT-546 (24-100 Mc) AS-541 (75-170 Mc) AT-197, GR (168-352 Mc) AN ART 13A-75 FT WIRE AT-544 (0.55 Mc-42 Mc) AT-543 (38-135 Mc) AT-545 (125-300 Mc)	AN ARR-7 0 55-42 Mc IN 6 BANDS AN APR-4Y 38-1000 Mc(4 BANDS), AN ARR-8B BROAD BAND UHF HIGH SPEED SCANNING RECEIVER (70-300 Mc IN 2 BANDS)	OUTPUT T-464, ALT-7 70W CW AND 60W NOISE MODULATED CW T-465, ALT-7 150W CW, MINIMUM 100W NOISE MODULATED CW AN ART-13A-100 WATTS REQUIRED POWER IS FURNISHED BY A POWER GROUP (25 kw AT 117 202V, 60 cps 4 WIRE, 3 PHASE 400 CYCLE MOTOR GENERATOR AND OTHER ASSOCIATED EQUIPMENT)		3 SYSTEMS BUILT DELIVERED TO TAC JUNE 1955
SE BARRAGE NG AND SE	NOISE POWER RF RANDOM NOISE FROM INTERNAL NOISE GENERATOR OR OTHER TYPE RF SIGNALS FROM EXTERNAL SOURCES	TUNED BYPASS AMPLIFIERS DRIVEN BY AN INTERNAL NOISE SOURCE	2 MODIFIED AS 161 ART WHIP ANTENNAS, VSWR OVER ENTIRE BAND IS LESS THAN 7 1 AND NEAR MID FREQ IS LESS THAN 3 1		OUTPUT AVERAGE 50W, VARIABLE 5-50 WATTS REQUIRED 8 AMPS, 115V, 300-1000 cps, SINGLE PHASE 10 AMPS 28 VDC		PRODUCTION AF 33(604)12400
VHF FRE-CEIVES AND ENT PRO-MMUNI-	AM-FM NOISE MODULATIONS	SWEPT, HAS FREQUENCY LOCK-ON FEATURE TWO 4 x 250 s, ONE SECOND JAMMING TIME	MODIFIED AT-190-B	SWEPT SENSITIVITY 2 MICROVOLTS WITH 10 db SIGNAL TO NOISE RATIO, SUPERHETERODYNE BANDWIDTH 25 kc	OUTPUT: 100-190W REQUIRED 1300 va AT 115V, 380-1000 cps, SINGLE PHASE AND 100W AT 28 VDC		PRODUCTION AF 33(604)18811
ICH SWEEP-SS THE NELS THE IABLE RE-SECOND SET-	NOT GIVEN	DIVIDED INTO 5 CHANNELS STOPS 2 5 SECONDS ON FREQUENCY TO BE JAMMED	UNKNOWN	SWEPT RECEIVER	OUTPUT: 20 WATTS PER CHANNEL REQUIRED UNK		
IED TO JAM IS WITH AN M MODU A MODIFI-	AM WITH NOISE, 6 Mc BANDWIDTH, FM WITH NOISE IN THE RF FREQUENCY RANGE OF 150-350 Mc WITH THE USE OF MODIFICATION KIT MX-527 APQ-2	T 9 APQ 2	NOT KNOWN	NONE	OUTPUT: 15 WATTS REQUIRED 115V AT 400-2600 cps SINGLE PHASE AND 28 VDC		PRODUCTION HXS-28261

SECRET

SECRET

FIG 16 - U S JAMMING EQUIPMENT (CONT'D)

EQUIPMENT	COGNIZANT SERVICE	FREQUENCY (MC)	FUNCTIONAL DESCRIPTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA
AN CRT 2	USAF	97.7 IN SEVEN BANDS	EXPENDABLE, AIR TRANSPORTABLE, SPARK-GAP EMISSION JAMMER FOR OPERATIONS AGAINST CW AND NOISE COMMUNICATIONS UNITS MAY BE DROPPED FROM STANDARD BOMB RACKS	CW OR NOISE	SPARK-GAP EMISSION	TRAILING WIRE OR WHIP
QRC-18(T) (AN/ALT-7 MODIFICATION)	USAF	24-350	RETROFIT OF AN/ALT-7 FOR FREQUENCY SWEEP CAPABILITIES COMPATIBLE WITH NEED FOR COMMUNICATIONS JAMMING.		AN/ALT-7	DEPENDENT UPON TYPE OF AIRCRAFT AND FREQUENCY BAND

1

SECRET

SECRET

FIG 16 - U S JAMMING EQUIPMENT (CONT'D)

PTION	JAMMING MODULATIONS	TRANSMITTER	ANTENNA	RECEIVER	POWER OUTPUT AND POWER REQUIRED	LOOK THRU	REMARKS
ABLE. FOR NOISE BE B RACKS	CW OR NOISE	SPARK-GAP EMISSION	TRAILING WIRE OR WHIP		OUTPUT 1 5-4 WATTS REQUIRED BATTERY OPERATED 4-5 HOUR LIFE		ORDER NUMBER 1148-MPD-45
FREQUENCY IBLE WITH JAMMING.		AN/ALT-7	DEPENDENT UPON TYPE OF AIRCRAFT AND FREQUENCY BAND	AN/APR-8 OR AN/APR-4	REQUIRED 115V. 380-1000 cps. 1.45 kva, SINGLE PHASE. 115V. 280-420 cps. 10 va, SINGLE PHASE. 28 VDC. 250W		11 AN/ALT-7 SETS MODIFIED AF 33(800) 26117

2

SECRET

FIG. 17 - RADIO NET JAMMING CAPABILITIES/SOVIET NETS AND U.S. JAMMERS/

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (KM)	RADIO TRANSMITTING MODE	REMARKS
MOTORIZED RIFLE (MR) COMPANY COMMAND NET	R-118 TO R-118 OR R-106 TO R-118	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS, QRC-22(T), AN/ALO-33	47.0-51.0	AM	0.1-0.5 W	0-1(200 M)	VOICE	NORMAL NET INVOLVES R-117 ONLY BUT COMPANY HQ MAY USE R-106 WHEN INCREASED RANGE IS NECESSARY. COMPANY R-106 NORMALLY IN BN COMMAND NET.
		AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS	48.1-48.8	AM	0.5-0.8 W	0-3(800 M)	VOICE	
TANK COMPANY COMMAND NET	10RT TO 10RT OR R-113 TO R-113	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	0-1(300 M)	VOICE	R-113 REPLACING 10RT IN COMPANY NETS. TWO JAMMERS WOULD BE NEEDED TO INSURE JAMMING OF THESE NETS.
		AN/ARQ-10, AN/ALT-3, AN/MLQ-22 (XE-1)	28.0-22.375	AM	0.0-10.0 W	0-1(300 M)	VOICE	
MR BN PRI-MARY CMD NET	R-106 TO R-106	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS	48.1-48.8	AM	0.5-0.8 W	0-3 (2)	VOICE	PRIMARYLY EMPLOYED DURING DIS-MOUNTED OPNS.
MR BN MOBILE OPERATIONS COMMAND NET	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	0-5 (3)	VOICE	BN AND COMPANIES USE RADIO MOUNTED ON BN APC'S (10RT BEING REPLACED BY R-113) OR BN MAY USE R-114 TO CALL UP BN APC'S
	R-113 TO R-113 OR	AN/ARQ-10, AN/ALT-3, AN/MLQ-22 (XE-1)	28.0-22.375	AM	0.0-10.0 W	0-5 (3)	VOICE	
	R-114 TO R-113	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-10 (T)	IN 28.0-30.0 RANGE	AM	1.0-2.0 W	0-5 (3)	VOICE	
MR BN TANK-INF COORDINATION NET	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	0-3 (2)	VOICE	PRIMARY USE BY BN IS COORDINATION AND COMMAND OF SUPPORTING TANK ELEMENTS. USES SAME RADIOS AS BN MOBILE OPERATIONS COMMAND EXCEPT OUTSTATIONS ARE IN SUPPORT TANKS. NET ELEMENTS ALSO USED BY BN COMPANIES TO COMMUNICATE WITH TANKS.
	R-113 TO R-113 OR	AN/ARQ-10, AN/ALT-3, AN/MLQ-22 (XE-1)	28.0-22.375	AM	0.0-10.0 W	0-3 (2)	VOICE	
	R-114 TO R-113	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-10 (T)	IN 28.0-30.0 RANGE	AM	1.0-2.0 W	0-3 (2)	VOICE	
MR BN FIRE SUPPORT COORDINATION NET	R-106 TO R-106	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS	48.1-48.8	AM	0.5-0.8 W	0-3 (1)	VOICE	USUALLY DIFFERENT FREQUENCY THAN BN PRIMARY COMMAND NET BUT ENABLES BN COMPANIES TO COMMUNICATE WITH BN FIRE SUPPORT ELEMENTS. EACH FIRE SUPPORT BATTERY ELEMENT HAS R-118 NET W/SUBORDINATE PLATOONS.
TANK BN PRI-MARY CMD NET**	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	0-5 (3)	VOICE	R-112 REPLACING 10RT AT BN HQ. TWO JAMMERS MAY BE NEEDED TO INSURE JAMMING OF THESE NETS.
	R-112 TO R-113	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-10 (T)	IN 28.0-48.8 RANGE	AM	UP TO 20.0 W	0-5 (3)	VOICE	
TANK BN ALTERNATE COMMAND**	R-105 TO R-105	AN/ARQ-10/QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS	35.95-48.15	FM	1.3 W	0-5 (3)	VOICE	EMPLOYED FOR BN COMPANY COMMUNICATIONS WHEN CO'S NOT USING TANKS.
TANK BN SUPPORT COORDINATION NET	R-106 TO R-106 OR	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T), BAS	48.1-48.8	AM	0.5-0.8 W	0-5 (2)	VOICE	EMPLOYED BY BN FOR COORDINATION WITH SUPPORTED INF AND OTHER ELEMENTS EQUIPPED WITH R-106 OR R-118.
	R-106 TO R-118	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-10(T) BAS	48.1-48.8	AM	0.5-0.8 W	0-5 (2)	VOICE	

* FIRST ECHELON UNITS ONLY. SECOND ECHELON AND OPERATIONAL RESERVE UNITS WILL NOT EMPLOY RADIO FOR COMMUNICATIONS PRIOR TO COMMITMENT. AVERAGE DISTANCE APART OF NET ELEMENTS IS SHOWN IN BRACKETS.

** ASSAULT BN AND TANK DIVISION PROBABLY EMPLOYS SIMILAR NETS.

SECRET

FIG 17 - RADIO NET JAMMING CAPABILITIES SOVIET NETS AND U S JAMMERS (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
MR REGT PRIMARY COMMAND NET	R-104 TO R-104	AN ARQ-10, AN CRT-2, QRC-8(T), QRC-13(T), AN ALT-3	1.5-4.75	AM	UP TO 20 W	1 TO 7 (5)	VOICE, CW	PRIMARYLY USED FOR CONTROL PRIOR TO BREAKTHROUGH AND PURSUIT.
MR REGT ALTERNATE COMMAND	R-105 TO R-105	AN ARQ-10, QRC-13(T), AN ALT-3, AN MLQ-22(XE-1), AN ALT-7, QRC-18(T)	35.95-46.15	FM	1.3 W	1 TO 7 (5)	VOICE	
MR REGT MOBILE OPERATIONS COMMAND NET	10RT TO 10RT OR	AN ARQ-10, AN CRT-2, QRC-8(T), QRC-13(T), AN ALT-3, AN MLQ-22(XE-1)	3.75-6.0	AM	5.0-6.0 W	1 TO 12 (7)	VOICE	R-112 TO R-113 MAY BE R-114 TO R-113 AND WOULD BE USED IN EITHER CASE FOR REGT TO COMMUNICATE WITH INDIVIDUAL ELEMENTS OF REGT'L RECON COMPANY OR WITH INDIVIDUAL TANKS. R-114 TO R-114 IS UNLIKELY TO BE USED. THIS NET IS USED WHEN PARTICIPANTS ARE OPERATING FROM TANKS AND APC'S.
	R-114 TO R-112 OR	AN ARQ-10, QRC-13(T), AN ALT-3, AN MLQ-22(XE-1), AN ALT-7, QRC-18(T)	IN 20.0-30.0 RANGE	AM	1.0-2.0 W	1 TO 12 (7)	VOICE	
	R-114 TO R-114 OR	AN ARQ-10, QRC-13(T), AN ALT-3, AN MLQ-22(XE-1), AN ALT-7, QRC-18(T)	IN 20.0-30.0 RANGE	AM	1.0-2.0 W	1 TO 12 (7)	VOICE	
	R-112 TO R-112 OR	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	IN 20.0-40.0 RANGE	AM	UP TO 20 W	1 TO 12 (7)	VOICE	
	R-112 TO R-113	AN ARQ-10, QRC-13(T), AN ALT-3, AN MLQ-22(XE-1), AN ALT-7, QRC-18(T)	IN 20.0-40.0 RANGE	AM	UP TO 20 W	1 TO 12 (7)	VOICE	
MR REGT ARTY COMMAND NET	R-105 TO R-105 OR	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	35.95-46.15	FM	1.3 W	1 TO 8 (3)	VOICE	R-105 TO R-105 IS FOR ORGANIC REGT'L ARTY. R-105 TO R-108 FOR ATTACHED ARTY.
	R-105 TO R-108	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	35.95-46.15	FM	1.3 W	1 TO 8 (3)	VOICE	
MR REGT AAA COMMAND NET	R-114 TO R-112 OR	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	IN 20.0-30.0 RANGE	AM	1.0-2.0 W	3 TO 20 (5)	VOICE	R-114 TO R-112 MAY BE R-112 TO R-112 AND WOULD BE FOR MOBILE OPERATIONS.
	R-109 TO R-109	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	21.15-28.3	FM	1.2 W	3 TO 20 (5)	VOICE	
MR REGT HQ COORDINATION NET	R-104 TO R-104	AN ARQ-10, AN CRT-2, QRC-8(T), QRC-13(T), AN ALT-3	1.5-4.75	AM	UP TO 20.0 W	1 TO 15 (5)	VOICE, CW	SPECIAL LINK SOMETIMES USED TO CONNECT ALL REGT'L HQ INSTALLATION INCLUDING REAR.
MR REGT LIAISON NET	R-105 TO R-105	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	35.95 TO 46.15	FM	1.3 W	1 TO 5 (12)	VOICE	LINK WHICH MAY BE ESTABLISHED BY EXTERNAL REGT OF DIV ON RIGHT WITH ADJACENT REGT OF ANOTHER DIV ON LEFT.
MR REGT REAR SERVICES NET	R-105 TO R-105	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	35.95-46.15	FM	1.3 W	3 TO 15 (7)	VOICE	OUTSTATIONS INCLUDE HQ, OF SUB-ORDINATE MR AND TANK BNS, ARTY AND AA ELEMENTS. REGT'L REAR IS NET CONTROL. LINK MAY INCLUDE REGT'L SAPPER COMPANY.
TANK REGT PRIMARY COMMAND NET	R-104 TO R-104	AN ARQ-10, AN CRT-2, QRC-8(T), QRC-13(T), AN ALT-3	1.5-4.75	AM	UP TO 20 W	0 TO 10 (5)	VOICE, CW	
TANK REGT ALTERNATE COMMAND NET	R-105 TO R-105	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	35.95-46.15	FM	1.3 W	0 TO 10 (5)	VOICE	
TANK REGT MOBILE OPERATIONS COMMAND NET	10RT TO 10RT OR	AN ARQ-10, AN CRT-2, QRC-8(T), QRC-13(T), AN ALT-3, AN MLQ-22(XE-1)	3.75-6.0	AM	5.0-6.0 W	0 TO 30 (5)	VOICE	R-112 REPLACING 10RT. TWO JAMMERS WILL BE NEEDED TO INSURE JAMMING UNTIL REPLACEMENT COMPLETE.
	R-112 TO R-112	AN ARQ-10, QRC-13(T), AN MLQ-22(XE-1), AN ALT-7, QRC-18(T), AN ALT-3	IN 20.0-40.0 RANGE	AM	UP TO 20 W	0 TO 30 (5)	VOICE	

SECRET

FIG. 17 - RADIO NET JAMMING CAPABILITIES/SOVIET NETS AND U.S. JAMMERS/ (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
TANK REGT ARTY COMMAND NET	R-105 TO R-105 OR	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), AN/ALT-3	35.95-48.15	FM	1.3 W	1 TO 10 (3)	VOICE	USE OF R-105 AND R-108 SAME AS NR REGT. USE OF R-112 TO R-112 OR R-113 IS FOR CONTROL OF ASSAULT GUN BATTERY. TANK BNS MAY USE SIMILAR NET FOR COORDINATION W/ASSULT GUN BTRY.
	R-105 TO R-108 OR	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), AN/ALT-3	35.95-48.15	FM	1.3 W	1 TO 10 (3)	VOICE	
	R-112 TO R-112/113	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), AN/ALT-3	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	1 TO 10 (3)	VOICE	
TANK REGT REAR SERVICES NET	R-104 TO R-104 OR	AN/ARQ-10, AN/CRT-2, QRC-8(T) QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	5 TO 25 (10)	VOICE	DIFFERENT STUDIES SHOW THIS NET AS R-104 OR R-105. LATTER PROBABLY ACCURATE.
	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), AN/ALT-3	35.95-48.15	FM	1.3 W	5 TO 25 (10)	VOICE	
REGT REN CO PRIMARY COMMAND NET**	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T) QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	** (2)	VOICE	10RT BEING REPLACED BY R-112 AND/OR R-113
	R-112 TO R-113 OR	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), AN/ALT-3	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	** (2)	VOICE	
	R-113 TO R-113	AN/ARQ-10, AN/ALT-3, AN/MLQ-22 (XE-1)	20.0-22.375	AM	8.0-10.0 W	** (2)	VOICE	
REGT ARTY BATTERY FIRE CONTROL NET ***	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), WAS	35.95-48.15	FM	1.3 W	0 TO 8 (500 M)	VOICE	
	R-108 TO R-108	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	27.8-38.35	FM	1.2 W	0 TO 8 (500 M)	VOICE	
REGT ASSAULT GUN BATTERY FIRE CONTROL NET****	R-112 TO R-113 OR	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7 QRC-18 (T)	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	0 TO 10 (300M)	VOICE	R-112 AND/OR R-113 REPLACING 10RT. R-113 MOST LIKELY.
	R-113 TO R-113 OR	AN/ARQ-10, AN/ALT-3, AN/MLQ-22 (XE-1)	20.0-22.375	AM	8.0-10.0 W	0 TO 10 (300M)	VOICE	
	10RT TO 10RT	AN/ARQ-10, AN/CRT-2, QRC-8(T), AN/ALT-3, AN/MLQ-22(XE-1), QRC-13 (T)	3.75-8.0	AM	5.0-8.0 W	0 TO 10 (300M)	VOICE	
REGT AAA BN COMMAND NET*****	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	3 TO 30 (3)	VOICE	10RT BEING REPLACED BY R-112 AND/OR R-113. ALL REGT'L AAA AND AANG ELEMENTS SELF-PROPELLED.
	R-112 TO R-113	AN/ARQ-10, QRC-13(T), AN/ALT 3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	3 TO 30 (3)	VOICE	
REGT AAA BTRY FIRE CONTROL NET*	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-18(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-8.0 W	3 TO 30 (1)	VOICE	10RT BEING REPLACED BY R-113. BOTH AA AND AANG ELEMENTS SELF-PROPELLED.
	R-113 TO R-113	AN/ARQ-10, AN/ALT 3, AN/MLQ-22 (XE-1)	20.0-22.375	AM	8.0-10.0 W	3 TO 30 (1)	VOICE	
NR DIV PRIMARY COMMAND NET	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	1 TO 15 (8)	VOICE, CW	

* COMMON TO BOTH NR AND TANK REGT. HOWEVER, BATTERY WITH NR REGT SUBORDINATE TO REGT'L AAA BN WHEREAS BATTERY SUBORD TO TANK REGT IS DIRECTLY SUBORDINATE TO REGT. BOTH SPAA AND AANG BATTERY OF NR REGT AA BN EMPLOY SIMILAR 10RT OR R-113 NET.

** OPERATING ZONE MAY EXTEND UP TO 15 km FORWARD OF THE REGT'L FRONT LINES.

*** APPLIES ONLY TO 120-mm/MORTAR, 107-mm RECOILLESS RIFLE, AND 85-mm SPAT BATTERIES OF NR REGT.

**** APPLIES ONLY TO 122/152-mm ASSAULT GUN BATTERY OF TANK REGT.

***** APPLIES ONLY TO AAA BN OF NR REGT

SECRET

FIG. 17 - RADIO NET JAMMING CAPABILITIES/ SOVIET NETS AND U.S. JAMMERS (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
MR DIV ALTERNATE COMMAND NET	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), MAS	35.95-48.15	FM	1.3 W	1 TO 15 (8)	VOICE	
MR DIV STAFF NET	R-118 TO R-118 R-104 OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	1.0-7.5	AM: FSK	50.0-100.0 W	4 TO 15 (8)	VOICE, CW RTT	AVAILABLE TOE INDICATES R-118 TO R-104 IS NORMAL NET W/WR REGT AND R-118 TO R-118 IS NORMAL NET W/TANK REGT. SOME INDICATION THAT R-103 NET IS USED (OUTSTATIONS MAY USE R-118 OR R-104) WHERE INCREASED RANGE IS NECESSARY.
	R-103 TO R-103	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3 AN/MLQ-22 (XE-1)	1.0-8.0	AM: FSK	120 W	5 TO 100 (20)	VOICE, CW RTT	
MR DIV MOBILE OPNS COMMAND NET	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-6.0 W	0 TO 30 (15)	VOICE	10RT BEING REPLACED BY R-112. SOME REPORTS INDICATE FORMER USE OF R-118 AT DIVISION TO PROVIDE INCREASED RANGE.
	R-112 TO R-112	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0 TO 40.0 RANGE	AM	UP TO 20.0 W	0 TO 30 (15)	VOICE	
MR DIV ARTY GP PRIMARY CMD NET*	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	5 TO 20 (8)	VOICE, CW	ALSO APPLICABLE TO REGT AND ARMY ARTY GROUP.
MR DIV ARTY GP ALTERNATE CMD NET*	R-108 TO R-108	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	27.8-38.35	FM	1.2 W	5 TO 20 (8)	VOICE	ALSO APPLICABLE TO REGT AND ARMY ARTY GROUP.
MR DIV ARTY GP STAFF NET*	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	5 TO 20 (8)	VOICE, CW	ALSO APPLICABLE TO REGT AND ARMY ARTY GROUP.
MR DIV AAA GP PRIMARY COMMAND NET**	R-109 TO R-109	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	21.15-28.3	FM	1.2 W	5 TO 50 (10)	VOICE	ARMY AAA GROUPS PROBABLY USE R-118 OR RADIO RELAY.
MR DIV AAA GP SPAA COMMAND NET**	R-112 TO R-113	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0 40.0 RANGE	AM	UP TO 20.0 W	3 TO 15 (10)	VOICE	USED FOR MOBILE CONTROL OF SPAA ONLY.
MR DIV AAA GP AIR DEFENSE COORDINATION NET**	R-109 TO R-109	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	21.15-28.3	FM	1.2 W	3 TO 20 (8)	VOICE	USED FOR COORDINATION BETWEEN DIV AND REGT AAA ELEMENTS.
DIV RECON BN PRIMARY COMMAND NET***	R-112 TO R-112 OR	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	**** (3)	VOICE	10RT BEING REPLACED BY R-112 AND/OR R-113. PROBABLE R-112 TO R-113 NET WILL PREVAIL.
	R-112 TO R-113 OR	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0-40.0 RANGE	AM	IN 20.0-40.0 RANGE	**** (3)	VOICE	
	10RT TO 10RT	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-8.0	AM	5.0-6.0 W	**** (3)	VOICE	
DIV RCN BN ALTERNATE COMMAND NET***	R-114 TO R-114	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0-30.0 RANGE	AM	1.0-2.0 W	**** (3)	VOICE	
DIV RCN BN AUXILIARY COMMAND NET***	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), MAS	35.95 48.15	FM	1.3 W	**** (3)	VOICE	
<p>* EMPLOYED BY DIV ARTY REGT FOR COMMAND AND STAFF WHEN REGT HQRS IS NOT DESIGNATED AN ARTY GROUP HEADQUARTERS.. ARTY OF TANK DIV EMPLOY SIMILAR NETS.</p> <p>** EMPLOYED BY DIV AAA REGT FOR CMD AND STAFF WHEN REGT HQRS IS NOT DESIGNATED A DIV AAA GROUP HEADQUARTERS. AAA OF TANK DIV EMPLOYS SIMILAR NETS.</p> <p>*** THESE UNITS ARE COMMON TO BOTH MR AND TANK DIVS.</p>								

FIG. 17 - RADIO NET JAMMING CAPABILITIES/SOVIET NETS AND U.S. JAMMERS/ (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
DIV SAPPER BN COMMAND NET***	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), WAS	35.95-46.15	FM	1.3 W	2 TO 15 (5)	VOICE	EACH PONTON BRIDGE PLATOON OF BN HAS TWO R-118.
DIV ARTY BN FIRE CONTROL NET***	R-108 TO R-108	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	27.8-36.35	FM	1.2 W	1 TO 10 (5)	VOICE	APPLICABLE TO NON-DIV ARTY BNS ALSO.
DIV ARTY BTRY FIRE CONTROL NET***	R-108 TO R-108	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	27.8-36.35	FM	1.2 W	0 TO 10 (4)	VOICE	APPLICABLE TO BTRY OF NON-DIV ARTY BNS ALSO.
DIV ARTY RECON NET*	R-108 TO R-108	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	27.8-36.35	FM	1.2 W	0 TO 10 (4)	VOICE	INTERNAL NET OF DIV ARTY INSTRUMENTAL RECON BTRY. INDIVIDUAL ELEMENTS MAY TIE INTO DIV ARTY GROUP ALTERNATE COMMAND NET OR INTO DIV ARTY BN FIRE CONTROL NETS.
TANK DIV PRIMARY COMMAND NET	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	2 TO 30 (10)	VOICE, CW	
TANK DIV ALTERNATE COMMAND NET	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), WAS	35.95-46.15	FM	1.3 W	2 TO 30 (10)	VOICE	
TANK DIV STAFF NET	R-118 TO R-118/104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	1.0-7.5	AM FSK	50.0-100.0 W	5 TO 30 (10)	VOICE, CW RTT	ALL OUTSTATION R-118 EXCEPT ASSAULT GUN BN AND POSSIBLE MR REGT. NO PRESENT INDICATIONS OF USE OF R-103 OR R-102 BY DIV.
TANK DIV MOBILE OPERATIONS COMMAND NET	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.75-6.0	AM	5.0-6.0 W	2 TO 40 (15)	VOICE	10RT BEING REPLACED BY R-112. SOME REPORTS INDICATE USE OF R-118 AT DIV TO PROVIDE INCREASED RANGE.
	R-112 TO R-112	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7 QRC-18 (T)	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	2 TO 40 (15)	VOICE	
TANK DIV COORDINATION NET	10RT TO 10RT OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	3.74-6.0	AM	5.0-6.0 W	0 TO 20 (8)	VOICE	10RT BEING REPLACED BY R-112. PRINCIPAL USE OF NET IS COORDINATION BETWEEN DIV ELEMENTS.
	R-112 TO R-112	AN/ARQ-10, QRC-13(T), AN/ALT-3, AN/MLQ-22(XE-1), AN/ALT-7, QRC-18 (T)	IN 20.0-40.0 RANGE	AM	UP TO 20.0 W	0 TO 20 (8)	VOICE	
TANK DIV HQRS LIAISON NET	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T) WAS	35.95-46.15	FM	1.3 W	2 TO 25 (8)	VOICE	
TANK DIV ENG AND CHEM NET	R-105 TO R-105	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), WAS	35.95-46.15	FM	1.3 W	2 TO 15 (8)	VOICE	
TANK DIV AIR LIAISON NET	R-824 TO R-801	QRC-13(T), AN/MLQ-22(XE-1), AN/ALT-7, QRC-18(T), AN/ALQ-33, AN/ALT-12, AN/SPT-3, AN/SPT-1, QRC-65(T), VHF COM JAMMER, AN/ARC-1, TX, -1A	100.0-150.0	AM	400.0 W	LINE OF SIGHT	VOICE	EMPLOYED BY AIR LIAISON ELEMENTS DETACHED TO DIVISION.

* MR DIV ONLY
 ** REPORTEDLY CAN BE JAMMED BY AN GLQ-3.
 *** THESE UNITS ARE COMMON TO BOTH MR AND TANK DIVS.
 **** OPERATING ZONE MAY EXTEND UP TO 50 km FORWARD OF THE DIV'S FRONT LINES. FIRE CONTROL NETS FOR MR AND TANK DIV ROCKET LAUNCHER ELEMENTS PROBABLY SIMILAR.

SECRET

FIG. 17 - RADIO NET JAMMING CAPABILITIES/SOVIET NETS AND U.S. JAMMERS/ (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
TANK DIV ARTY PRIMARY COMMAND NET	R-104 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	2 TO 20 (8)	VOICE, CW	
TANK DIV ARTY ALTERNATE COMMAND NET	R-100 TO R-100	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	27.8-36.35	FM	1.2 W	2 TO 20 (8)	VOICE	
TANK DIV ARTY STAFF NET	R-110 TO R-110 OR	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3, AM/MLQ-22 (XE-1)	1.0-7.5	AM	50.0-100.0 W	5 TO 20 (8)	VOICE, CW RTT	OUTSTATIONS PROBABLY USE R-110 OR R-104 AS AVAILABLE.
	R-110 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3, AM/MLQ-22 (XE-1)	1.0-7.5	AM	50.0-100.0 W	5 TO 20 (8)	VOICE, CW	
TANK DIV RESERVE NET	R-104 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	0 TO 30 (10)	VOICE, CW	SAME AS NR DIV.
TANK DIV REAR SERVICES NET	R-104 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	10 TO 40 (25)	VOICE, CW	REAR HQ ONLY.
TANK DIV ARTY/AAA COMMAND NET	R-109 TO R-109	AM/ARQ-10, QRC-13(T), AM/ALT-3, AM/MLQ-22(XE-1), AM/ALT-7, QRC-18 (T)	21.15-28.3	FM	1.2 W	2 TO 30 (10)	VOICE	SAME AS NR DIV.
NR DIV COORDINATION NET	10RT TO 10RT OR	AM/ARQ-10, AM/CRT-2, QRC-18(T), QRC-13(T), AM/ALT-3, AM/MLQ-22 (XE-1)	3.75 8.0	AM	5.0-8 W	1 TO 15 (8)	VOICE	10RT BEING REPLACED BY R-112. PRINCIPAL USE OF NET IS COORDINATION BETWEEN DIVISION ELEMENTS.
	R-112 TO R-112	AM/ARQ-10, QRC-13(T), AM/ALT-3, AM/MLQ-22(XE-1), AM/ALT-7, QRC-18 (T)	1N 20.0-40.0 RANGE	AM	UP TO 20.0 W	1 TO 15 (8)	VOICE	
NR DIV HQ LIAISON NET	R-104 TO R-104 OR	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	2 TO 35 (12)	VOICE, CW	NET VARIOUSLY REPORTED AS R-104 OR R-105. R-105 MOST LIKELY.
	R-105 TO R-105	AM/ARQ-10, QRC-13(T), AM/MLQ-22 (XE-1), AM/ALT-7, QRC-18(T), WAS	35.95-46.15	FM	1.3 W	2 TO 35 (12)	VOICE	
NR DIV ENGR AND CHEM NET	R-105 TO R-105	AM/ARQ-10, QRC-13(T), AM/MLQ-22 (XE-1), AM/ALT-7, QRC-18(T), WAS	35.95-46.15	FM	1.3 W	0 TO 20 (8)	VOICE	NET SOMETIMES SHOWN AS R 104.
NR DIV EXTERNAL COORDINATION NET	R-104 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	10 TO 15 (30)	VOICE, CW	
NR DIV AIR OBSERVATION NET	R-800 SERIES TO R-801	QRC-13(T), AM/MLQ-22(XE-1), AM/ALT-7, QRC-18(T), AM/ALQ-33, AM/ALT-12, AM/SPT-3, AM/SPT-1, QRC-65(T), VHF COM JAMMER, AM/ARC-1, -1X, -1A; TDY-1	100.0-150.0	AM	UNKNOWN	LINE OF SIGHT	VOICE	NET EMPLOYED BY ORGANIC DIV LIGHT AIRCRAFT OR HELICOPTORS.
NR DIV AIR LIAISON NET	R-824 TO R-801	QRC-13(T), AM/MLQ-22(XE-1), AM/ALT-7, QRC-18(T), AM/ALQ-33, AM/ALT-12, AM/SPT-3, AM/SPT-1, QRC-65(T), VHF COM JAMMER, AM/ARC-1, -1X, -1A; TDY-1	100.0-150.0	AM	400.0 W	LINE OF SIGHT	VOICE	EMPLOYED BY AIR LIAISON ELEMENTS DETAILED TO DIVISION
NR DIV ARTY PRIMARY COMMAND NET	R-104 TO R-104	AM/ARQ-10, AM/CRT-2, QRC-8(T), QRC-13(T), AM/ALT-3	1.5-4.75	AM	UP TO 20.0 W	2 TO 20 (8)	VOICE, CW	
NR DIV ARTY ALTERNATE COMMAND NET	R-100 TO R-100	AM/ARQ-10, QRC-13(T), AM/MLQ-22 (XE-1), AM/ALT-7, QRC-18(T)	27.8-36.35	FM	1.2 W	2 TO 20 (8)	VOICE	
* NR DIV ONLY								
** REPORTEDLY CAN BE JAMMED BY AN/GLQ-3.								

SECRET

FIG. 17 - RADIO NET JAMMING CAPABILITIES/SOVIET NETS AND U.S. JAMMERS/ (CONT'D)

TYPE SOVIET NET	RADIOS USED NET CONTROL TO OUTSTATION	PRESENT US JAMMING CAPABILITIES	RADIO FREQUENCY RANGE (Mc)	RADIO MODULATION	RADIO POWER	RADIO NORMAL ZONE OF OPERATIONS FROM LOC (km)	RADIO TRANSMITTING MODE	REMARKS
MR DIV ARTY STAFF NET	R-118 TO R-118 OR	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3, AN/MLQ-22 (XE-1)	1.0-7.5	AM/FSK	50.0-100.0 W	5 TO 20 (8)	VOICE, CW, RTT	VARIOUSLY REPORTED AS ALL R-118, ALL R-104, AND R-118 TO R-104. MOST PROBABLE NET CONTROL USES R-118 AND OUTSTATIONS USE R-118 OR R-104 AS AVAILABLE.
	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	5 TO 20 (8)	VOICE, CW	
	R-118 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), AN/ALT-3, AN/MLQ-22(XE-1)	1.0-7.5	AM	50.0-100.0 W	5 TO 20 (8)	VOICE, CW	
	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	1 TO 15 (10)	VOICE, CW	
MR DIV RADIO RELAY NET	R-401 TO R-403	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T), QRC-22(T), AN/ALQ-33, AN/ALT-12	66.0-69.975	FM	1.0 TO 5.0 W	3 TO 15 (8)	VOICE, INVERTED VOICE, RTT, FACSIMILE	NOW ESTABLISHED IN STATIC SITUATION ONLY. LATER MAY BE STANDARD FOR ALL OPNS. EMPLOYED FOR COMMAND AND STAFF COMMUNICATIONS DIV TO SUBORDINATE REGT. R-401M OPERATES BELOW 66.0 Mc.
MR DIV ARTY/AAA COMMAND NET	R-109 TO R-109	AN/ARQ-10, QRC-13(T), AN/MLQ-22 (XE-1), AN/ALT-7, QRC-18(T)	21.15-28.3	FM	1.2 W	2 TO 20 (8)	VOICE	EMPLOYED FOR COORDINATION BETWEEN DIV ARTY HQ AND DIV AAA REGT HQS OR AAA GROUP HQS.
MR DIV REAR SERVICES NET	R-104 TO R-104	AN/ARQ-10, AN/CRT-2, QRC-8(T), QRC-13(T), AN/ALT-3	1.5-4.75	AM	UP TO 20.0 W	10 TO 40 (20)	VOICE, CW	REAR HQ ONLY

SECRET

FIG. 18 -(S) ESTIMATED EFFECTIVENESS OF JAMMING AND ICD AGAINST SELECTED SOVIET GROUND UNITS

TYPE OF UNIT (ARM)	COMPANY (BATTERY) AND LOWER ECHELON	BATTALION	REGIMENT (BRIGADE)	DIVISION	ARMY
MOTORIZED RIFLE	JAMMING - POOR TO FAIR ICD - FAIR TO GOOD	JAMMING - FAIR TO GOOD ICD - POOR TO FAIR	JAMMING - POOR TO FAIR ICD - POOR	JAMMING - POOR ICD - POOR	JAMMING - POOR ICD - POOR
TANK	JAMMING - FAIR TO GOOD ICD - FAIR TO GOOD	JAMMING - GOOD TO VG ICD - FAIR TO GOOD	JAMMING - FAIR TO GOOD ICD - POOR TO FAIR	JAMMING - FAIR ICD - POOR	JAMMING - POOR ICD - POOR
AIRBORNE RIFLE	JAMMING - GOOD TO VG ICD - GOOD TO VG	JAMMING - GOOD TO EXCL ICD - GOOD TO VG	JAMMING - GOOD TO VG ICD - FAIR TO GOOD	JAMMING - FAIR ICD - FAIR	JAMMING - NA ICD - NA
RECONNAISSANCE	JAMMING - FAIR TO GOOD ICD - FAIR TO GOOD	JAMMING - GOOD TO VG ICD - FAIR TO GOOD	JAMMING - NA ICD - NA		
ARTILLERY	JAMMING - GOOD TO EXCL. ICD - FAIR TO GOOD	JAMMING - FAIR TO GOOD ICD - POOR TO FAIR	JAMMING - POOR TO FAIR ICD - POOR	JAMMING - POOR ICD - POOR	JAMMING - NA ICD - NA
ANTI-AIRCRAFT ARTILLERY	JAMMING - GOOD TO EXCEL ICD - FAIR TO GOOD	JAMMING - GOOD TO VG ICD - POOR TO FAIR	JAMMING - FAIR TO GOOD ICD - POOR	JAMMING - NA ICD - NA	
SURFACE TO SURFACE MISSILE	JAMMING - NA ICD - NA	JAMMING - NA ICD - NA	JAMMING - GOOD TO EXCL ICD - POOR TO FAIR	JAMMING - NA ICD - NA	
SABOTAGE INTELLIGENCE AND LONG-RANGE AGENT	JAMMING - VG TO EXCL ICD - GOOD TO VG	JAMMING - NA ICD - NA			

SECRET